PLANTEAMIENTO DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 PARA LA EMPRESA DE SERVICIOS DE TECNOLOGÍA SITECH DE COLOMBIA SAS EN LOS PROCESOS GESTIÓN FINANCIERA, GESTIÓN DE LOGÍSTICA Y GESTIÓN DE IT

KEVIN ORLANDO LIZARAZO LOZANO

UNIVERSIDAD PILOTO DE COLOMBIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FACULTAD DE INGENIERÍA
BOGOTÁ D.C.
2016

PLANTEAMIENTO DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 PARA LA EMPRESA DE SERVICIOS DE TECNOLOGÍA SITECH DE COLOMBIA SAS EN LOS PROCESOS GESTIÓN FINANCIERA, GESTIÓN DE LOGÍSTICA Y GESTIÓN DE IT

KEVIN ORLANDO LIZARAZO LOZANO

Trabajo de grado para optar al título de
Especialista en Seguridad informática

Asesor Temático
Juan Carlos Alarcón Suescun
Magíster en seguridad de la información

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FACULTAD DE INGENIERÍA
BOGOTÁ D.C.
2016

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C. 27 de Agosto de 2016

DEDICATORIA

En primer lugar a Dios, por quien estoy hoy aquí y quien me ha dado las mayores bendiciones a mi vida, Mi esposa quien me motiva a ser mejor cada día, mis padres y mi hermana quienes me ayudaron a crecer como una persona íntegra, y a toda mi familia que han sido de apoyo en cada paso de mi vida.

Kevin Orlando Lizarazo Lozano

AGRADECIMIENTOS

Expreso especial agradecimiento a mi esposa, quien me motivo a seguir estudiando y tuvo paciencia durante las largas jornadas de trabajo, a los profesores quienes compartieron sin límites sus concomimientos y nos motivaron par ser mejores en cada labor asignada y por ultimo a mi tutor quien me guio a paso a paso en la elaboración de este proyecto.

CONTENIDO

pág.

LISTA DE FIGURAS

LISTA DE CUADROS

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: es todo aquello referente a la información que tiene valor para la compañía y es necesario protegerlo, este puede ser de tipo primario o de soporte.

DOFA: análisis de Debilidades, Oportunidades, Fortalezas y Amenazas**,** es una metodología de estudio para diagnosticar una empresa, proyecto o área. [1]

GPO: abreviatura de *Group Policy Object*, que en español significa, Directivas de grupo, la cual es simplemente la forma más sencilla de alcanzar y configurar opciones de usuario y de equipo en redes basadas en servicios de dominio de directorio activo.[2]

ISP: siglas de Proveedor de Servicios de Internet, se refiere al operador o empresa que suministra el servicio de internet.

POAM: abreviatura utilizada para referirse a Perfil de Oportunidades y Amenazas en el Medio, el cual se utiliza para realizar análisis externo.[3]

PCI: abreviatura utilizada para referirse al Perfil de Capacidad Interna, el cual se utiliza para realizar el análisis interno.[4]

RIESGO: probabilidad de que una amenaza explote una vulnerabilidad de un activo de información generando un impacto negativo para la organización.

SOA: por las siglas en Ingles de *Statement of Applicability* un documento que si bien es un requisito de documentación en el estándar ISO/IEC 27001, puede ser utilizado por cualquier organización, como una manera de mantener el registro y control de las medidas de seguridad que son aplicadas.[5]

SGSI: abreviatura utilizada para referirse a un Sistema de Gestión de Seguridad de la información, es el equivalente a las siglas en ingles ISMS que se refieren a *Information Security Management System*.

TI/IT: se refiere a Tecnologías de la información, y hace referencia al área encargada de gestionar y administrar los servicios tecnológicos en una compañía, comúnmente llamado “Sistemas”.

---

[1] Humberto Serna Rodríguez. Gerencia Estratégica, Teoría – Metodología – Alineamiento, implementación y mapas estratégicos, 3R Editores, Edición 10, 2015, pág. 185

[2] Microsoft. Centro de Ti de Windows. [En línea]. Disponible en: https://technet.microsoft.com/es-es/library/hh147307(v=ws.10).aspx [Actualizado en Abril de 2011]

[3] Humberto Serna Rodríguez. Gerencia Estratégica, Teoría – Metodología – Alineamiento, implementación y mapas estratégicos, 3R Editores, Edición 10, 2015, pág. 150

[4] Humberto Serna Rodríguez. Gerencia Estratégica, Teoría – Metodología – Alineamiento, implementación y mapas estratégicos, 3R Editores, Edición 10, 2015, pág. 168

[5] ESET. Seguridad Corporativa. [En línea]. Disponible en: http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/ [Publicado el 1 de Abril de 2015]

RESUMEN

El siguiente documento es una presentación del planteamiento de un sistema de gestión de seguridad de la información para la empresa Sitech de Colombia S.A., específicamente en los procesos de gestión financiera, gestión logística y gestión de IT. Aunque Sitech es una empresa pequeña en personal realiza intercambios comerciales de gran tamaño, esto gracias a sus alianzas estratégicas y contactos con empresas importantes de Bogotá.

El inventario de activos, amenazas, vulnerabilidades, impactos y probabilidades de ocurrencia se realizó en compañía de los dueños o responsables de los procesos y activos, quienes están en la capacidad de realizar cada valoración.

Como resultado de este planteamiento de SGSI se determinó que la mayoría de los riesgos a los que está expuesto Sitech se deben a falta de procedimientos, políticas y controles de verificación diseñados, implementados y documentados, adicional a la falta de un programa de concienciación para el personal de la empresa.

Es por esto que se recomienda el diseño e implementación de varios controles de la norma ISO 27001:2013 así como un plan de entrenamiento periódico para disminuir la probabilidad de ocurrencia de los riesgos identificados.

INTRODUCCIÓN

No es novedad que para las empresas la información se convirtió en uno de sus activos más importantes, y los esfuerzos por proteger esta información generaron la necesidad de crear estándares y procedimientos normalizados. Desde las grandes multinacionales hasta las pequeñas empresas, e incluso nosotros como personas nos preocupamos porque la información sensible no esté al alcance de cualquier persona que pueda hacer uso indebido de nuestros datos. Cuando queremos hacer un intercambio comercial con alguna otra persona tenemos los mayores cuidados, comprobamos más de una vez si la otra persona es confiable y muchas veces con temor, realizamos transacciones en internet esperando que no seamos víctimas de un fraude, en donde nuestros datos queden expuestos a merced de algún atacante malintencionado.

Las empresas que se dedican a vender servicios de tecnología son puestas a prueba cuando se quiere delegar en ellos la administración y configuración de sus servidores, data center, redes de comunicación y bases de datos. Por lo anterior los dueños y gerentes de las organizaciones buscan un aliado confiable y seguro, que cumpla con la normatividad vigente y entregue un plus adicional en la seguridad de la información.

En este proyecto encontrará el planteamiento de un sistema de gestión de seguridad de la información para una empresa dedicada a la integración de servicios de tecnología, buscando identificar los riesgos latentes de sus activos y el plan de tratamiento de riesgos de los mismos. Este es un paso importante en el camino de la gestión de la seguridad de la información en toda compañía que busca consolidarse como un socio estratégico y confiable, con ventajas competitivas ante las demás empresas del mercado.

1. PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

El auge actual de la seguridad de la información, ataques informáticos a grandes empresas, violación de la seguridad de cuentas a personajes famosos, robo de información entre organizaciones abre las puertas para que empresas se dediquen a prestar servicios de consultoría en seguridad de la información. Pero muchas de estas empresas se crean para prestar servicios de seguridad de la información sin tener implementado en su interior un SGSI, o por lo menos políticas de seguridad de la información, estas empresas pueden estar en desventaja al no implementar las soluciones que quieren vender y pueden dar a entender a sus usuarios que no cumplen con la normatividad vigente para proteger la propiedad intelectual e información sensible de clientes y proveedores.

Sitech de Colombia SAS es una empresa dedicada a la venta de equipos de tecnología, soluciones de comunicaciones e infraestructura tecnológica, dentro de sus ventajas competitivas tiene el compromiso con la calidad en el servicio. Sitech quiere aumentar su ventaja competitiva contando con un sistema de gestión de seguridad de la información que les dé la confiabilidad a sus clientes y proveedores de encontrar un socio estratégico de negocio que se preocupa por la integridad, confidencialidad y disponibilidad en sus soluciones.

¿Cómo puede Sitech de Colombia SAS proteger de manera adecuada sus objetivos de negocio para asegurar el aprovechamiento de nuevas oportunidades en el mercado actual?

1.2 JUSTIFICACIÓN

Día a día más empresas buscan estar certificados en seguridad de la información ISO27001:2013, lo cual hace que sus socios estratégicos deban cumplir con las políticas establecidas en su sistema de gestión de seguridad de la información.

Identificar las vulnerabilidades propias de los activos de información de una compañía puede ayudarle a entender las exigencias y necesidades de los prospectos de asociados de negocio. Adicional, para Sitech de Colombia es importante cuidar sus activos más importantes, los cuales son la información de relaciones de negocios durante más de 5 años, documentación de implementaciones de servicios e infraestructura, configuraciones de servidores y data center. Proteger estos activos de información justifica la necesidad de garantizar la confidencialidad, integridad y disponibilidad mediante el planteamiento de un sistema de gestión de seguridad de la información.

2 OBJETIVOS

2.1 GENERAL

Diseñar un SGSI basado en la norma ISO 27001:2013 para la empresa Sitech de Colombia SAS en los procesos de gestión financiera, gestión de logística y gestión de IT.

2.2 ESPECÍFICOS

Realizar el análisis diferencial de la seguridad de la información en los procesos de gestión financiera, gestión de logística y gestión de IT, comparando la situación actual con los requisitos de ISO 27001:2013, definiendo el alcance del SGSI para Sitech de Colombia SAS.

Definir una política de seguridad de la información que esté alineada con los objetivos estratégicos de la organización y que cumpla con la normatividad vigente y requerimientos contractuales relativos a la seguridad de la información.

Diseñar el plan de gestión de riesgos de los activos de información para los procesos de gestión financiera, gestión de logística y gestión de IT, planteando controles, políticas y recomendaciones que garanticen la confidencialidad, integridad y disponibilidad de la información.

3. MARCO REFERENCIAL

3.1 DESCRIPCIÓN DE LA COMPAÑÍA

Sitech de Colombia SAS fue fundada en Abril de 2010 por el señor José Heriberto Ceballos y Natalia Díaz en la ciudad de Bogotá, inicialmente estuvo ubicada en Rincón de Salitre, Carrera 59 # 57a-26, en estas oficinas iniciaron 3 personas con la línea de negocio de tóner para impresoras. Dado el conocimiento y experiencia de sus fundadores el catálogo de servicios creció a medida que se dieron a conocer en el entorno tecnológico, para las diferentes empresas en la capital. Sitech se hace representante y canal directo de varias marcas reconocidas a nivel mundial y sumado al compromiso con la calidad del servicio le permiten convertirse en el socio estratégico de prestigiosas compañías.

El catálogo de servicios de Sitech se describe a continuación:

- Administración e implementación de plataformas tecnológicas.
- Dimensionamiento, arquitectura, consultoría y soluciones de infraestructura.
- Soluciones de virtualización.
- *Outsourcing* de impresión: Tracking, autenticación y políticas de impresión y administración.
- Mantenimiento de computadores, impresoras, actualización de equipos y migración de imágenes.
- Diseño, planeación e instalación de cableado estructurado.
- *Renting* tecnológico.
- Soluciones de audio y video.
- Gestión de IT basada en ITIL.
- Biometría.

De los productos que ofrece Sitech se destacan:

- Equipos de computación.
- Impresoras y Escáner.
- Servidores.
- Almacenamiento.
- Conectividad.
- Potencia y protección eléctrica.
- Telefonía y comunicaciones.
- Video profesional.
- suministros e impresión.
- Venta de periféricos.
- Sistemas POS.
- Climatización.

3.1.1 Misión. Somos una empresa colombiana especializada en proveer soluciones integrales de tecnología, que brinda a sus clientes altos niveles de valor agregados basados en puntualidad, responsabilidad, calidad y acompañamiento. Contamos con alianzas estratégicas, infraestructura requerida y personal idóneo para asegurar nuestra oferta de servicios, dentro de los principios éticos y legales.

3.1.2 Visión. Ser líderes en el mercado nacional, siendo reconocidos como un aliado estratégico tecnológico de nuestros clientes, convirtiéndonos en su socio de confianza.

3.1.3 Valores corporativos. Los valores corporativos de Sitech son:

- Compromiso con los clientes.
- Alegría.
- Integridad.
- Excelencia en el servicio.
- Respeto.
- Honestidad y Transparencia.

3.2 ANÁLISIS DE SU ENTORNO

Para realizar el análisis del entorno en Sitech de Colombia SAS se encuesto una muestra de 7 personas del personal de la compañía, con el fin de realizar el diagnostico interno y externo de la misma. Este diagnóstico se ejecutó con base en el libro de gerencia estratégica de Humberto Serna Gómez, los capítulos 5, 6 y 7 sirvieron de guía para determinar el estado actual de Sitech.

La encuesta fue diligenciada en línea por colaboradores de Sitech, ingresando al formulario web de la herramienta Qualtrics en el url https://qtrial2016q2.az1.qualtrics.com/SE/?SID=SV_7agKS0Nwmg1enVH.

3.2.1 Análisis Externo. Aunque Sitech de Colombia SAS es una empresa que solo tiene 6 años desde que se fundó, ha tenido excelentes relaciones comerciales con grandes empresas en la ciudad Bogotá, lo cual le ha permitido capitalizarse y tomar ventaja de las variables externas, económicas, sociales y culturales que la rodean.

Adicional Sitech es una empresa que sabe utilizar la tecnología y está a la vanguardia de las estrategias de negocio que ayudan a catapultarla como una empresa líder en el mercado. El mundo avanza a un paso agigantado que exige a las empresas adaptarse con rapidez cambiando la forma de hacer negocios, tanto así que muchas grandes empresas que dominaban el mundo hace unos años, hoy no existen pues no se adaptaron al cambio.

El resultado de la encuesta de análisis interno realizada a una muestra comprendida por la alta dirección de Sitech y algunos empleados se muestra en el anexo A. Este análisis está basado en el POAM, el perfil de Oportunidades y Amenazas del Medio. Capítulo 5 del Libro “Gerencia Estratégica de Humberto Serna Gómez”.

El perfil de oportunidades y amenazas del medio de Sitech se resume en el cuadro 1. POAM Sitech, el cual se muestra a continuación:

Cuadro 1. POAM Sitech

Oportunidades	**Amenazas**
1. Crecimiento del mercado en torno a la tecnología	1. Patrones y cambios en el mercado
2. Estilos de vida tecnológicos	2. Tasa de cambio de moneda extranjera fluctuante
3. Oportunidades en el sector educativo	3. Competencia desleal
Fuente: Autor	

3.2.2 Análisis Interno. Es importante recordar que identificar debilidades ayuda para que el Análisis DOFA de la organización tenga un mejor resultado, tener debilidades no significa que las cosas se estén haciendo mal, pero siempre se puede mejorar, y tenemos siempre áreas por mejorar. Los sistemas de gestión se basan en la mejora continua y aunque no se crea tener debilidades en la organización, siempre tendremos puntos o áreas más débiles que otras en las que debemos trabajar, es por esto que se solicitó a los empleados que diligenciaran la encuesta con objetividad y sin temor a expresarse sinceramente, en el punto de vista de cada uno de ellos se pudo encontrar opciones de mejora para Sitech.

El resultado del análisis interno de Sitech de Colombia SAS se encuentra detallado en el Anexo B con la tabulación obtenida mediante la metodología de PCI, perfil de capacidad interna. Sin embargo a continuación se muestra el perfil de capacidad interna condensado en el cuadro 2. PCI Sitech.

Cuadro 2. PCI Sitech

Fortalezas	**Debilidades**
1. Habilidad para responder a la tecnología Cambiante 2. Agresividad para enfrentar la competencia 3. Nivel tecnológico de la empresa 4. Estabilidad laboral y nivel de pertenencia de la fuerza de trabajo 5. Lealtad y satisfacción del cliente 6. Facilidad de créditos y acuerdos de pago con proveedores	1. Falta de sistemas de control 2. Alta Rotación de personal 3. Falta de inversión de I&D de nuevos servicios 4. Estabilidad de los costos
Fuente: Autor	

3.2.3 Análisis DOFA. El análisis DOFA permite identificar como la empresa sacara provecho de las oportunidades y fortalezas trabajando en mejorar las debilidades, superando las amenazas, para lograr generar una propuesta de valor que los diferencia de las demás empresas del mercado que pueden llegar a ser sus competidores. En el Cuadro 3. DOFA Sitech se puede observar el resultado de dicho análisis.

Cuadro 3. DOFA Sitech

	Oportunidades	**Amenazas**
Análisis DOFA SITECH	1. Crecimiento del mercado en torno a la tecnología. 2. Estilos de vida tecnológicos. 3. Oportunidades en el sector educativo.	1. Patrones y cambios en el mercado. 2. Tasa de cambio de moneda extranjera fluctuante. 3. Competencia desleal.
Fortalezas	**Estrategias FO**	**Estrategias FA**
1. Habilidad para responder a la tecnología Cambiante. 2. Agresividad para enfrentar la competencia. 3. Nivel tecnológico de la empresa. 4. Estabilidad laboral y nivel de pertenencia de la fuerza de trabajo. 5. Lealtad y satisfacción del cliente. 6. Facilidad de créditos y acuerdos de pago con proveedores.	1. Implementar estrategias de negocio para nichos de mercado en crecimiento. 2. Aprovechar la lealtad de los clientes para generar estabilidad y dedicar esfuerzo en incursionar en el sector educativo. 3. Generar un acercamiento a los prospectos de clientes mediante el uso de tecnología aprovechando el uso masivo de las redes sociales.	1. Generar planes de acción mediante el uso delos créditos y acuerdos de pagos a proveedores para superar la fluctuación de la moneda extranjera. 2. Fortalecer y socializar la ética en los empleados y clientes evitando los impactos de la competencia desleal. 3. Generar estrategias tecnológicas de cambio para responder oportunamente a las variaciones y requerimientos del mercado.
Debilidades	**Estrategias DO**	**Estrategias DA**
1. Falta de sistemas de control. 2. Alta Rotación de personal. 3. Falta de inversión de I&D de nuevos servicios. 4. Estabilidad de los costos.	1. Realizar pruebas piloto de tecnología con el personal internos, para motivarlos a conocer la línea de negocio, aprovechando el auge de la tecnología en los estilos de vida actuales. 2. Implementar las soluciones del sector educativo internamente para incentivar la I&D de nuevos servicios y capacitar al personal en general en el uso de las mismas. 3. Generar estrategias generales para estabilizar los costos de operación al contemplar el crecimiento de la organización junto con el del mercado.	1. Generar sistemas de control y verificación de procesos 2. Definir procesos documentados que le permita al personal generar estándares en busca de costos mínimos de reprocesos. 3. Implementar planes de incentivos para evitar la alta rotación de personal y la migración a la competencia.
Fuente: Autor		

3.3 BENEFICIOS PARA LA EMPRESA DEL SGSI

Son muchos los beneficios para Sitech de Colombia de un sistema de gestión de seguridad de la información, los dos principales pueden ser; la confianza que pueden tener sus clientes al saber que se gestionan los riesgos identificando las vulnerabilidades de los activos de información, los cuales pueden ser atacados por diferentes amenazas que podrían impactar seriamente la organización. El beneficio económico es consecuente con la identificación y gestión de riesgos mencionada anteriormente, pues se pueden reducir los costos vinculados a los incidentes de seguridad de la información.

Adicional a estos beneficios y dado que la información es un activo muy importante para toda organización se puede mencionar:

Se reduce la probabilidad de que se produzcan perdidas de información en la organización.

Mejora continua en los procesos y análisis contante de riesgos para la organización.

Minimizar los riesgos en materia de confidencialidad, integridad y disponibilidad.

Procesos con metodología sistemática que le permite a la organización tomar decisiones para las actuaciones necesarias en la reducción natural de los peligros para los activos de información, ejecutando controles continuos sobre los riesgos.

3.4 BENEFICIOS DE ADOPTAR EL ESTÁNDAR ISO27001

Sitech de Colombia maneja información confidencial de muchas empresas y entidades importantes de Bogotá y Colombia, muchas de ellas con presencia a nivel nacional, es por esto que adoptar el estándar ISO 27001 trae consigo el beneficio del aumento de credibilidad y confianza por parte de sus clientes, al saber que en cumplimiento con la norma se debe establecer una cultura de la seguridad y una excelencia en el tratamiento de la información de todos los procesos del negocio incluidos en el alcance de la implementación. Adicional a este beneficio se pueden considerar los siguientes:

Facilidad de integración con otros sistemas de gestión normalizados tales como ISO 9001, 14001, 18001 entre otros.

Voluntad de cumplimiento de la legislación y normatividad vigente incluyendo y sin limitarse a información personal y propiedad intelectual.

Asegurar la continuidad de operación del negocio y de los procesos de seguridad de la información.

Sensibilización del personal de la organización en la correcta manipulación de la información y la importancia de aplicar las medidas de seguridad adecuadas para cada uno de los responsables de la manipulación de la información o los dueños de los activos de información.

4. DISEÑO METODOLÓGICO

4.1 DIAGNOSTICO DE SEGURIDAD DE LA EMPRESA

4.1.1 Análisis de Brecha ISO27001. El análisis de brecha ISO 27001 en Sitech de Colombia S.A. se realizó con la ayuda de la herramienta web de 27001 Academia, al cual se puede acceder desde el url http://advisera.com/27001academy/es/herramientas/herramienta-gratuita-analisis-de-brecha-para-iso-27001/.

El diagnóstico del estado actual con respecto al estado requerido por Sitech se realizó en dos fases; entrevistas a miembros de los procesos incluidos en el alcance, incluyendo el personal de IT y el análisis de similitudes en las respuestas a las entrevistas.

Esta herramienta permite validar de manera fácil y en compañía de los dueños de proceso, la alta gerencia y el área de IT, cada uno de los controles y aspectos requeridos por la norma ISO 27001:2013.

Una vez finalizadas las entrevistas se procedió a consolidar la información para generar un estado general, comparando las respuestas de los diferentes entrevistados y acercando más a la realidad la situación actual de la compañía, a continuación se describe el resultado general del análisis de brecha.

4.1.1.1 Contexto de la organización.

- Conocimiento de la organización y su contexto.

¿La organización determina los fines del SGSI?
R. Sí.

¿La organización determina las cuestiones internas y externas que son pertinentes para la finalidad de SGSI?
R. No.

¿Determina la organización cómo las cuestiones internas y externas podrían influenciar en la capacidad del SGSI para conseguir los resultados previstos?
R. No.

- Comprensión de las necesidades y expectativas de las partes interesadas.

¿La organización determina las partes interesadas?
R. Sí.

¿Existe la lista de todos los requisitos de las partes interesadas?
R. No.

- Determinar el alcance del SGSI.

¿El alcance está documentado con los límites claramente definidos?
R. No.

- Sistemas de gestión de información de seguridad.

¿Han establecido, documentado, implementado, mantenido y mejorado continuamente un sistema de gestión de seguridad de información según los requisitos de la norma ISO 27001?
R. No.

4.1.1.2 Liderazgo.

- Liderazgo y compromiso.

¿Los objetivos generales del SGSI son compatibles con la dirección estratégica?
R. No.

¿La dirección garantiza los recursos necesarios para el SGSI cuando sea necesario?
R. No.

¿La dirección asegura que el SGSI logra sus resultados previstos?
R. No.

- Política.

¿Existe una política de seguridad de la información con objetivos definidos o un marco para el establecimiento de objetivos?
R. No.

¿La política de seguridad de información está documentada y es comunicada dentro de la empresa y a otras partes interesadas?
R. No.

- Roles, responsabilidades y autoridades en la organización.

¿Están asignadas y comunicadas los roles, responsabilidades y autoridades para la seguridad de la información?
R. No.

4.1.1.3 Planificación.

- Acciones para tratar riesgos y oportunidades.

- Generalidades.

¿Las cuestiones internas y externas, así como los requisitos de las partes interesadas, son consideradas al abordar los riesgos y las oportunidades?
R. No.

- Valoración de riesgos de seguridad de la información.

¿Hay un proceso documentado para identificar los riesgos de seguridad de la información, incluyendo los criterios de aceptación del riesgo y criterios de evaluación del riesgo?
R. No.

- Tratamiento de riesgos de la seguridad de la información

¿Está documentado el proceso de tratamiento del riesgo, incluyendo las opciones de tratamiento del riesgo y cómo crear una declaración de aplicabilidad?
R. No.

- Objetivos de seguridad de la información y planes para lograrlos.

¿Los objetivos de seguridad de la información son establecidos en las funciones relevantes de la organización, medido en su práctica y coherente con la política de seguridad de la información?
R. No.

¿Existe un plan, o conjunto de planes, para lograr los objetivos de seguridad de la información incluyendo responsabilidades, método de evaluación y tiempos para el plan?
R. No.

4.1.1.4 Soporte.

- Recursos.

¿Se proporcionan los recursos adecuados para todos los elementos del SGSI?
R. No.

- Competencia.

¿Es evaluada la competencia, y la capacitación donde sea necesario, para el personal que realiza tareas que puedan afectar a la seguridad de la información? ¿Los registros de competencias son mantenidos?
R. No.

- Concienciación.

¿El personal es consciente de la política de seguridad de la información, de su papel y las consecuencias de no cumplir con las normas?
R. No.

- Comunicación.

¿Hay un proceso de comunicación relacionado con la seguridad de la información, incluyendo las responsabilidades, qué se comunica, a quién y cuándo?
R. No.

- Información documentada (7.5.1 General; 7.5.2 Creación y actualización; 7.5.3 Control de información documentada)

¿La documentación del SGSI incluye la política de seguridad de la información, objetivos, el alcance del SGSI, los principales elementos y su interacción, documentos y registros de la norma ISO 27001 y aquellos identificados por la empresa?
R. No.

¿Se asegura que existe un manejo de documentos y registros, incluyendo quién revisa y aprueba los documentos, cómo y dónde se publican, almacenan y protegen?
R. No.

¿Es controlada la información documentada de origen externo?
R. Sí.

4.1.1.5 Operación.

- Planificación y control operacional.

¿La organización tiene la información documentada necesaria para estar segura de que sus procesos se llevan a cabo según lo planeado?
R. Sí.

¿Se controlan los cambios planificados? ¿Las consecuencias de cambios no planificados son revisadas para identificar acciones de mitigación?
R. No.

¿Los procesos tercerizados son identificados y controlados?
R. Sí.

- Apreciación de los riesgos de seguridad de información.

¿Los riesgos, sus propietarios, la probabilidad, las consecuencias y el nivel de riesgo son identificados? ¿Estos resultados se encuentran documentados?
R. No.

- Tratamiento de los riesgos de seguridad de información.

¿Existe un plan de tratamiento del riesgo, aprobado por los propietarios de riesgo?
R. No.

¿Hay una lista documentada con todos los controles necesarios, con el estado aplicación y justificación?
R. No.

4.1.1.6 Evaluación del desempeño.

- Seguimiento, medición, análisis y evaluación.

¿Está definido qué tiene que ser medido, a través de qué método, quien es responsable, y quien analizará y evaluará los resultados?
R. No.

¿Los resultados de medición son documentados, analizados y evaluados por personas responsables?
R. No.

- Auditoría Interna.

¿Existe un programa de auditoría que define las fechas, responsabilidades, reportes, criterios de auditoría y alcance?
R. No.

¿Las auditorías internas son realizadas según un programa de auditoría, los resultados se informan a través de un informe de auditoría interna y se levantan o identifican acciones correctivas?
R. No.

- Revisión por la dirección

¿La Revisión por dirección se realizada regularmente, y se documentan los resultados en actas de reunión?
R. No.

¿La dirección decide sobre todas las cuestiones cruciales importantes para el éxito del SGSI?
R. No.

4.1.1.7 Mejora.

- No conformidad y acciones correctivas.

¿La organización reacciona a cada no conformidad?
R. No.

¿La organización considera la eliminación de la causa de la no conformidad y, en su caso, toma medidas correctivas?
R. No.

¿Se registran todas las no conformidades, junto con las acciones correctivas?
R. No.

- Mejora continua.

¿El SGSI se ajusta continuamente para mantener su idoneidad, adecuación y eficacia?
R. No.

4.1.1.8 Anexo A de la norma ISO 27001:2013. (Nota: Deben ser implementados sólo los controles marcados como aplicable en la Declaración de Aplicabilidad.)

A.5 Políticas de seguridad
¿Existen políticas publicadas, aprobadas por la dirección, para apoyar la seguridad de la información?
R. No.

¿Las políticas de seguridad de la información son revisadas y actualizadas?
R. No.

A.6 Organización de la seguridad
¿Están definidas todas las responsabilidades de seguridad de la información?
R. No.

¿Los deberes y las responsabilidades son correctamente segregados teniendo en cuenta las situaciones de conflicto de intereses?
R. No.

¿Existen definidas contactos con las autoridades competentes?
R. Sí.

¿Existen definidos contactos con grupos de interés especial o asociaciones profesionales?
R. Sí.

¿Los proyectos consideran aspectos relacionados con la seguridad de la información?

R. Sí.

¿Existen definidas reglas para el manejo seguro de los dispositivos móviles?
R. No.

¿Existen reglas que definen cómo está protegida la información de la organización teniendo en cuenta el teletrabajo?
R. No.

A.7 Seguridad relativa a los recursos humanos

¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?
R. Sí.

¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de información?
R. No.

¿La dirección requiere activamente que todos los empleados y contratistas cumplan con las reglas de seguridad de la información?
R. No.

¿Los empleados y contratistas asisten a entrenamientos para realizar mejor sus tareas de seguridad, y existen programas de sensibilización?
R. Sí.

¿La organización tiene un proceso disciplinario?
R. No.

¿Existen acuerdos que cubren las responsabilidades de seguridad de información que siguen siendo válidas después de la terminación del empleo?
R. No.

A.8 Gestión de activos

¿Existe un inventario de activos?
R. No.

¿Todos los activos en el inventario de activos tienen un dueño designado?
R. No.

¿Existen definidas reglas para el manejo de activos y de información?
R. No.

¿Los activos de la organización son devueltos cuando los empleados y contratistas finalizan su contrato?
R. Sí.

¿Están definidos los criterios para clasificar la información?
R. No.

¿Existen procedimientos que definen cómo etiquetar y manejar información clasificada?
R. No.

¿Existen procedimientos que definen cómo manejar activos?

R. Sí.

¿Existen procedimientos que definen cómo manejar medios extraíbles en consonancia con las reglas de clasificación?
R. No.

¿Existen procedimientos formales para la eliminación de medios?
R. No.

¿Son protegidos los medios que contienen información sensible durante el transporte?
R. No.

A.9 Control de acceso

¿Existe una política de control de acceso?
R. No.

¿Los usuarios tienen acceso sólo a los recursos que se les permite?
R. Sí.

¿Los derechos de acceso son proporcionados mediante un proceso de registro formal?
R. No.

¿Existe un sistema de control de acceso formal para el inicio de sesión en sistemas de información?
R. No.

¿Los derechos de acceso privilegiado son manejados con especial cuidado?
R. Sí.

¿Las contraseñas, y otra información de autenticación secreta, son proporcionadas de forma segura?
R. Sí.

¿Los propietarios de activos comprueban periódicamente todos los derechos de acceso privilegiado?
R. Sí.

¿Los derechos de acceso son actualizados cuando hay un cambio en la situación del usuario (por ejemplo: cambio organizacional o terminación)?
R. Sí.

¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?
R. Sí.

¿El acceso a la información en los sistemas es restringido según la política de control de acceso?
R. No.

¿Es requerido un sistema de *login* en los sistemas según la política de control de acceso?
R. Sí.

¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma segura su información de autenticación?
R. Sí.

¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?
R. Sí.

¿El acceso al código fuente es restringido a personas autorizadas?
R. Sí.

A.11 Seguridad física y del entorno

¿Existen zonas seguras que protegen la información sensible?
R. Sí.
¿Es protegida la entrada a las zonas seguras?
R. No.

¿Las zonas seguras están ubicadas en un lugar protegido?
R. No.

¿Existen instaladas alarmas, sistemas de protección contra incendios y otros sistemas?
R. No.

¿Existen definidos procedimientos para las zonas seguras?
R. No.

¿Las zonas entrega y carga están protegidas?
R. Sí.

¿Los equipos son debidamente protegidos?
R. Sí.

¿Los equipos están protegidos contra las variaciones de energía?
R. Sí.

¿Están adecuadamente protegidos los cables de energía y telecomunicaciones?
R. Sí.

¿Existe mantenimiento de los equipos?
R. Sí.

¿La retirada de información y equipos fuera de la organización está controlada?
R. No.

¿Los activos de la organización son debidamente protegidos cuando no están en las instalaciones de la organización?
R. Sí.

¿Es correctamente eliminada la información de los equipos que se van a eliminar?
R. No.

¿Existen reglas para proteger los equipos cuando estos no estén siendo usados por los usuarios?
R. No.

¿Hay orientaciones a los usuarios sobre qué hacer cuando estos no están presentes en sus estaciones de trabajo?
R. No.

A.12 Seguridad de las operaciones

¿Están documentados los procedimientos de TI?
R. No.

¿Los cambios que podrían afectar a la seguridad de la información son estrictamente controlados?
R. No.

¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?
R. Sí.
¿Se separan los entornos de desarrollo, pruebas y producción?
R. No.

¿El software antivirus y otros programas para la protección de malware se instalan y utilizan correctamente?
R. Sí.

¿Existe una política de *backup* definida y se lleva a cabo correctamente?
R. Sí.

¿Los eventos relevantes de los sistemas son verificando periódicamente?
R. Sí.

¿Los registros están protegidos adecuadamente?
R. Sí.

¿Están adecuadamente protegidos los *logs* de los administradores?
R. Sí.

¿Está la hora de todos los sistemas de TI sincronizada?
R. Sí.

¿La instalación de software es estrictamente controlada?
R. No.

¿La información de análisis de vulnerabilidades es correctamente gestionada?
R. No.

¿Existen reglas para definir restricciones de instalación de software a los usuarios?
R. No.

¿Están las auditorías de sistemas de producción planeadas y se ejecutan correctamente?
R. No.

A.13 Seguridad de las comunicaciones

¿Las redes son gestionadas para proteger la información de sistemas y aplicaciones?
R. Sí.

¿Los requisitos de seguridad para servicios de red están incluidas en los acuerdos?
R. Sí.

¿Existen redes segregadas considerando los riesgos y la clasificación de los activos?
R. Sí.

¿Las transferencias de información están debidamente protegidas?
R. No.

¿Los acuerdos con terceras partes consideran la seguridad durante la transferencia de información?
R. No.

¿Los mensajes que se intercambian sobre las redes están protegidos correctamente?
R. No.

¿La organización posee una lista con todas las cláusulas de confidencialidad que deben ser incluidos en los acuerdos con terceros?

A.14 Adquisición, desarrollo y mantenimiento de sistemas de información

¿Se definen requisitos de seguridad para nuevos sistemas de información, o para cualquier cambio sobre ellos?
R. Sí.

¿La información de aplicaciones transferida a través de redes públicas es adecuadamente protegida?
R. Sí.

¿Las transacciones de información a través de redes públicas son adecuadamente protegidas?
R. Sí.

¿Existen definidas reglas para el desarrollo seguro de software y de los sistemas?
R. No.

¿Se controlan los cambios en los sistemas nuevos o existentes?
R. Sí.

¿Las aplicaciones críticas son debidamente probadas después de los cambios realizados en los sistemas operativos?
R. Sí.

¿Se realizan sólo los cambios necesarios a los sistemas de información?
R. Sí.

¿Los principios de ingeniería de sistemas seguros son aplicados al proceso de desarrollo de sistemas de la organización?
R. No.

¿Es seguro el entorno de desarrollo?
R. No.

¿Es monitorizado el desarrollo externalizado de sistemas?
R. No.

¿Los requisitos de implementación de seguridad son probada durante el desarrollo del sistema?
R. No.

¿Existe definido un criterio para aceptar los sistemas?
R. Sí.

¿Los datos de prueba son cuidadosamente seleccionados y protegidos?
R. Sí.

A.15 Relación con proveedores

¿Existe una política para el tratamiento de los riesgos relacionados con proveedores y socios?
R. No.

¿Los requisitos de seguridad son incluidos en los acuerdos con los proveedores y socios?
R. No.
¿Los acuerdos con los proveedores incluyen requisitos de seguridad?
R. No.
¿Son supervisados regularmente los proveedores?
R. Sí.

¿Los cambios relacionados con los acuerdos y contratos con proveedores y socios tienen en cuenta los riesgos existentes?
R. Sí.

A.16 Gestión de incidentes de seguridad de la información

¿Los incidentes son gestionados adecuadamente?
R. No.

¿Los eventos de seguridad son reportados adecuadamente?
R. No.

¿Los empleados y contratistas informan sobre las debilidades de seguridad?
R. No.

¿Los eventos de seguridad son evaluados y clasificados correctamente?
R. No.

¿Están documentados los procedimientos para dar respuesta a los incidentes?
R. No.

¿Se analizan los incidentes de seguridad correctamente?
R. No.

¿Existen procedimientos que definen cómo recopilar evidencias?
R. No.

A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

¿Existen definidos requisitos para la continuidad de la seguridad de la información?
R. No.

¿Existen procedimientos que aseguren la continuidad de la seguridad de la información durante una crisis o un desastre?
R. No.

¿Se realizan test y pruebas de continuidad?
R. No.

¿La infraestructura IT está redundada, incluyendo su planeamiento y operación?
R. No.

A.18 Cumplimiento

¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?
R. No.

¿Existen procedimientos para proteger los derechos de propiedad intelectual?
R. Sí.

¿Los registros están protegidos adecuadamente?
R. Sí.

¿La información personal está protegida adecuadamente?
R. Sí.

¿Se utilizan controles criptográficos correctamente?
R. Sí.

¿La seguridad de la información es revisada regularmente por un auditor independiente?
R. No.

¿Los gerentes revisan regularmente si las políticas de seguridad y procedimientos son llevados a cabo adecuadamente en sus áreas de responsabilidad?
R. No.

¿Los sistemas de información son revisados regularmente para comprobar su cumplimiento con los estándares y las políticas de seguridad de la información?
R. No.

4.1.2 Análisis de contexto de seguridad. Dado que Sitech actualmente no cuenta con un Sistema de Gestión de Seguridad de la Información documentado e implementado el resultado del análisis de brecha muestra en su gran mayoría incumplimiento en cada uno de los ítems evaluados con respecto a la norma ISO 27001. Sin embargo esto no quiere decir que Sitech no tenga en cuenta la seguridad de la información en sus procesos, pues ejecuta algunas actividades para minimizar riesgos en la seguridad de sus activos.

La mayoría de los controles de seguridad que implementa Sitech se hacen a nivel lógico en la red, la consola de administración del antivirus permite gestionar las reglas de firewall de cada uno de los computadores de la organización, realizando filtrado de paquetes en la navegación a internet, control de paquetes y puertos. La seguridad en los recursos compartidos se realiza por medio de grupos de seguridad del directorio activo y GPO's de controlador de dominio.

Actualmente Sitech se encuentra trabajando en la documentación de los procesos y procedimientos en cada una de las áreas de la compañía, esto se realiza como parte del compromiso de buscar la certificación de gestión de calidad ISO 9001:2015, sin embargo el hecho de que los procesos y procedimientos no estén totalmente documentados y socializados permite que se abra la oportunidad para cometer errores en la ejecución de las actividades diarias, adicional la falta de entrenamiento en seguridad de la información al personal permite que el recurso humano sea susceptible a amenazas tales como ingeniería social y *phishing*.

4.1.3 Análisis de necesidad de seguridad. La necesidad de la seguridad de la información impacta significativamente la mayoría de entes en el mundo, dado que la tecnología crece a pasos agigantados y cada vez se hace más necesaria en el diario vivir de cada individuo, esto permite que se abran oportunidades de explotación de vulnerabilidades para los atacantes, Quien está protegido de esto tiene una ventaja competitiva en el mercado lo cual puede ayudarlo a ser líder en

medio de su ámbito laboral. Es por esto que es importante identificar la necesidad de la seguridad de la información desde dos puntos de vista.

4.1.3.1 Cliente Interno. Muchas organizaciones identifican las necesidades de sus clientes externos con facilidad, pero dejan a un lado las necesidades de sus clientes internos, y es por estos clientes internos que avanza la organización, las necesidades de cada uno de estos es tan importante como las necesidades de aquellos a quienes se brindan los servicios y de quienes se recibe los ingresos.

Desde el punto de vista del cliente interno es necesaria la seguridad de la información porque esta brinda un ambiente seguro para el desempeño de las labores, así como garantiza que se toman en cuenta las medidas, reglamentación y normas necesarias para el tratamiento de su información confidencial y privada. El hecho de tener en cuenta un plan de continuidad del negocio da la tranquilidad de que se tienen en cuenta las precauciones necesarias para generar una estabilidad en el trabajo, identificándose, midiéndose y tratando los riesgos que puedan llegar a afectar la empresa y directamente la labor de un empleado.

4.1.3.2 Cliente externo. Durante este proyecto se ha explicado las ventajas para la compañía de tener un sistema de seguridad de la información implementado, lo cual impacta directamente en la percepción que tienen los clientes del manejo que se la va a dar a la información que se comparte en los negocios que se establezcan. Esto da punto de partida para decir que para el cliente externo que quiere que su información este protegida y que los productos y servicios que recibe cuenten con el plus de la seguridad, las empresas con las que establece vínculos comerciales son aquellas que tienen un SGSI implementado y una cultura de seguridad de la información establecida, generando para ellos beneficios tales como los mencionados en los numerales 2.3 y 2.4 de este mismo proyecto.

Dado que hoy en día la información es un activo muy importante no solo para las personas sino para los organismos en general, el tratamiento adecuado de su información es una prioridad para los clientes, por eso toman medidas internas para salvaguardar la información y se vinculan con entidades que busquen el mismo fin, haciendo necesario que la seguridad de la información este en cada movimiento que realizan.

4.2 DISEÑO DEL SGSI

4.2.1 Alcance del SGSI. El alcance del sistema de gestión de seguridad de la información está considerado para los procesos de Gestión Financiera, Gestión de Logística y Gestión de IT.

4.2.2 Política de seguridad de la información. A continuación se presenta la propuesta de política de seguridad de la información para la organización:

En Sitech de Colombia Reconocemos la importancia de proteger los activos de información de nuestros clientes, aliados estratégicos y empleados. Por lo tanto, estamos comprometidos con desarrollar, implementar y mejorar continuamente un sistema de seguridad de la información que identifique y proteja los activos de información de nuestra organización.

Identificaremos amenazas potenciales, al igual que impactos y vulnerabilidades de la información y de las facilidades en donde se procesa. Desarrollaremos procesos y procedimientos para identificar, minimizar y/o eliminar los riesgos de seguridad que puedan afectar los sistemas de información.

Brindaremos a todos los empleados de Sitech concienciación y entrenamiento sobre los procedimientos implementados en materia de seguridad de la información. Es responsabilidad de cada empleado preservar la confidencialidad, disponibilidad e integridad de los activos de

información que estén bajo su dominio, siguiendo las políticas y procedimientos desarrollados en el sistema de gestión de seguridad de la información.

Para asegurar la exactitud y protección de la información utilizada, alcanzaremos y mantendremos la certificación de nuestro sistema de gestión, con el fin de proteger los activos de información contra amenazas potenciales, así como para cumplir con la legislación, regulaciones, normas y estándares internacionales más relevantes relacionados con la seguridad de la información.

4.2.3 Roles y Responsabilidades de seguridad. Es muy importante que la alta dirección esté involucrada en el montaje del sistema de gestión de seguridad de la información, por lo tanto está debería ser participe en la determinación, asignación y compromiso de los roles y responsabilidades de seguridad de la información.

Es por esto que se determina que debe existir como mínimo para obtener buenos resultados del sistema de gestión de seguridad de la información los siguientes roles con sus responsabilidades.

Responsable de seguridad de la información: Es el responsable de planear, coordinar y administrar los procesos de seguridad informática en la organización, así como difundir la cultura de seguridad en todos los miembros de la organización, dentro de sus responsabilidades principales se puede destacar.

- Asegurar el buen funcionamiento del sistema de gestión de seguridad de la información.
- Guiar a la alta dirección ante incidentes de seguridad.
- Desarrollar procedimientos de seguridad que fortalezcan la política de seguridad de la información.
- Elaborar un plan de respuesta a incidentes.
- Coordinar la realización periódica de Auditorias de seguridad de la información.
- Mantener y aumentar el interés de la alta dirección en el sistema de gestión de seguridad de la información.

Sitech de Colombia Designa como responsable de seguridad de la información al Director de Infraestructura.

Comité de seguridad: Aunque Sitech es una empresa pequeña y está en camino a la certificación de sus procesos, podría existir un pequeño comité de seguridad de la información conformado por un representante de las áreas de la compañía, este comité estará compuesto por el Responsable de seguridad de la información, el gerente general, el contador como representante del área financiera y administrativa y el gerente comercial en representación de dicha área. Este comité tendrá bajo su responsabilidad las siguientes tareas entre otras:

- Aprobar las políticas de seguridad de la información, análisis de riesgos, normas y plan de continuidad de negocio.
- Promover los proyectos de seguridad de Sitech de Colombia S.A.S.
- Delimitar las responsabilidades de todo el personal involucrado en el Sistema de gestión de seguridad de la información.
- Aprobar los acuerdos de confidencialidad a utilizar el personal de la compañía y con terceras partes.
- Aprobar el plan de revisiones periódicas de seguridad de la información en la organización.
- Supervisar el plan de continuidad del negocio.
- Velar por el cumplimiento de la normatividad vigente en materia de seguridad de la información.

Personal de la empresa: Es muy importante que cada uno de los miembros de la compañía sea consciente que es parte fundamental en el proceso de seguridad de la información y gestión de riesgos, de cada uno de ellos depende el éxito del sistema de gestión de seguridad de la información, pues son responsables del cumplimiento de cada una de las políticas aprobadas por el comité de seguridad de la información, cerrando la brecha para que las amenazas no puedan explotar las vulnerabilidades de los activos de información. Este es el eslabón que debe ser más vigilado, pues las estrategias de los atacantes avanzan cada día para vencer la protección y capacitación que tiene cada empleado en las compañías, entre sus responsabilidades se puede encontrar:

- Informar al responsable de seguridad de la información cualquier sospecha de incumplimiento a las políticas de seguridad o amenaza latente.
- Cumplir con cada una de las políticas y normas, así como la política de seguridad de la información.
- Propender por actuar acorde al sistema de seguridad de la información en cada una de sus actividades.
- Procurar que se conserve la integridad, confidencialidad y disponibilidad de los sistemas de información de la compañía.
- Custodiar con especial cuidado las credenciales asignadas de acceso a los sistemas.
- Mantener en reserva cualquier debilidad en el sistema en materia de seguridad de la información.

4.2.4 Procedimiento de gestión de riesgos. El procedimiento de riesgos consiste básicamente en los siguientes pasos:

- Identificación de los activos de información
- Identificación de las vulnerabilidades de los activos de información
- Pruebas de vulnerabilidad
- Identificación de las amenazas que pueden explotar las vulnerabilidades
- Valoración de los activos de información
- Evaluación de riesgos
- Identificación de riesgos priorizados
- Niveles de aceptación del riesgo
- Elaborar la declaración de aplicabilidad
- Elaborar el plan de tratamiento de riesgos

La actividad de identificación de activos, vulnerabilidades y amenazas se realizó en compañía de cada uno de los empleados que pertenecen a los procesos de gestión financiera, gestión logística y gestión de IT. El dueño o responsable de cada activo es la persona más indicada para identificar las amenazas y vulnerabilidades de cada uno de estos, así como la valoración de cada activo basados en las variables de confidencialidad, integridad y disponibilidad en una escala de valor de 1 a 5, donde 1 es el valor más bajo y 5 es el valor más alto, un ejemplo de esta valoración es el siguiente:

1. Muy Bajo
2. Bajo
3. Medio
4. Alto
5. Muy alto

Los activos se identificaron de acuerdo a su tipo, ya sea primario o secundario tal como lo menciona el Anexo B de la norma ISO 27005. Los activos primarios identificados fueron aquellos

como actividades, procesos, procedimientos o la misma información. Los activos secundarios se dividieron en categorías tales como hardware, software, red, lugar, organización o persona.

El impacto que puede producir la afectación de un activo de información se valoró de acuerdo a 5 aspectos los cuales son legal, imagen corporativa, capacidad de recuperación, restricción de acceso y objetivos corporativos, el cuadro 4. Aspectos de valoración de impacto muestra el valor y la descripción de cada valor.

Cuadro 4. Aspectos de valoración de impacto

Aspectos	ID	Criterios	Descripción
Legal	1	Nulo	No se ve afectada la Empresa si este activo es comprometido o no se encuentra disponible.
	2	Bajo	Si los SLA's con los clientes se verán impactados por la disponibilidad o afectación del activo, pero no sobrepasa el nivel de aceptación
	3	Medio	La Empresa podría recibir quejas de los clientes por incumplimiento de los SLA's, derivadas de la disponibilidad o afectación de este activo de información.
	4	Alto	Un cliente podría penalizar a la Empresa por incumplimiento de los SLA's, derivados de la disponibilidad o afectación de este activo de información.
	5	Catastrófico	Cancelación de un contrato por incumplimiento de SLA's, derivado de la falta o afectación del activo.
Imagen corporativa	1	Nulo	No se ve afectada la imagen pública de la Empresa.
	2	Bajo	Algunos de las partes interesadas tienen percepciones negativas de la Empresa.
	3	Medio	Un grupo significativo de las partes interesadas se queja formalmente debido a la afectación / falta de disponibilidad de este activo.
	4	Alto	La Empresa es desprestigiada en medios de comunicación.
	5	Catastrófico	Cancelación del contrato derivado del desprestigio de la imagen de la Empresa
Interés & recuperación	1	Nulo	El activo de información no es del interés público y se puede recuperar a corto plazo
	2	Bajo	El activo de información no es del interés público, pero su recuperación sería a largo plazo
	3	Medio	El activo de información sí es del interés público y se puede recuperar a corto plazo
	4	Alto	El activo de información sí es del interés público y se requiere de un esfuerzo mayor para recuperarlo
	5	Catastrófico	El activo es de interés público y muy difícilmente se podría recuperar
Restricción de acceso	1	Nulo	El activo de información no se encuentra expuesto a acceso no autorizado
	2	Bajo	El activo de información se encuentra expuesto para su acceso, sólo al personal involucrado en el proceso
	3	Medio	El activo de información se encuentra expuesto para su acceso no autorizado por personal interno, no involucrado en el proceso
	4	Alto	El activo de información se encuentra expuesto para su acceso no autorizado, por personal externo
	5	Catastrófico	El activo se encuentra extremadamente expuesto para su acceso a personal externo e interno
Objetivos corporativos	1	Nulo	1. Los objetivos de la Empresa no se ven afectados.
	2	Bajo	2. Es probable que los objetivos de la Empresa se vean afectados.
	3	Medio	3. Si se compromete el activo o no se encuentra disponible, se retrasará el cumplimiento de los objetivos de la Empresa.
	4	Alto	4. Si se compromete el activo o no se encuentra disponible no se cumplirá con los objetivos de la Empresa.
	5	Catastrófico	5. Si se compromete el activo o no se encuentra disponible, se perderá la confianza de los inversionistas, proveedores y/o clientes.
Fuente: Autor			

Para valorar los riesgos fue necesario definir la probabilidad de ocurrencia del mismo, dado que el riesgo es el resultado de la operación entre el valor del impacto para la compañía si un activo es afectado contra la probabilidad de ocurrencia, para lo cual se definió la probabilidad de ocurrencia de acuerdo a la escala mostrada en el cuadro 5. Probabilidad de ocurrencia.

Cuadro 5. Probabilidad de ocurrencia

Probabilidad de ocurrencia		
Valor	**Descripción**	**Interpretación**
1	Improbable	Muy baja probabilidad
2	Poco probable	Baja probabilidad
3	Probable	Mediana probabilidad
4	Muy probable	Alta probabilidad
5	Altamente probable	Muy alta probabilidad
Fuente: Autor		

La lista de riesgos priorizados surgió de la calificación de cada riesgo, aquellos que tienen mayor valor significa que tienen mayor probabilidad de ocurrencia o su impacto para la organización es muy significativo, por lo cual deben ser los primeros en tratar.

Una vez identificados lo riesgos en la organización la alta gerencia definió el nivel de aceptación del riesgo, para lo cual se diseñó una matriz de niveles. La cual se puede observar en el cuadro 6. Matriz de niveles de aceptación del riesgo

Cuadro 6. Matriz de niveles de aceptación del riesgo

Impacto\Probabilidad		Improbable	Poco Probable	Probable	Muy Probable	Altamente Probable
		1	2	3	4	5
1	Nulo	1	2	3	4	5
2	Bajo	2	4	6	8	10
3	Medio	3	6	9	12	15
4	Alto	4	8	12	16	20
5	Catastrófico	5	10	15	20	25
Fuente: Autor						

Según esta matriz de niveles la dirección de Sitech determino que los niveles de aceptación del riesgo serán los que se muestran en el cuadro 7. Niveles de aceptación del riesgo.

Cuadro 7. Niveles de aceptación del riesgo

Nivel de aceptación	**Rango de Valores**
Aceptable	1 - 4
Moderado	5 - 9
Inaceptable	10 - 25
Fuente: Autor	

Una vez se identificaron los riesgos y niveles de aceptación del riesgo se puedo validar los controles de la norma ISO 27001 que aplican para los riesgos identificados en Sitech con cual se determinó la declaración de aplicabilidad.

El plan de tratamiento de riesgo consiste en definir los controles que se pueden aplicar para tratar los riesgos identificados, pero antes de definir los controles para tratar los riesgos se debieron identificar los controles existentes en la organización, esto para ahorrar esfuerzos y costos en tiempo y dinero. Una vez se identificaron los controles se valoraron para calcular el peso de los riesgos después de aplicar dichos controles.

4.3 ANÁLISIS DE RIESGOS DE SEGURIDAD

4.3.1 Lista de activos de información. Para realizar el inventario de activos de información en Sitech de Colombia se realizaron entrevistas a cada uno de los miembros de las áreas de Logística, Financiera e IT. Estos activos se catalogaron de acuerdo a su tipo, el cual según el anexo B de la norma ISO 27005 se dividen en primarios y de soporte. Los mismos fueron valorados de acuerdo a la triada de la seguridad de la información y al impacto que puede llegar a tener para la organización la afectación de cada uno de los mismos.

La figura 1. Muestra un ejemplo del formato utilizado para el inventario de activos de información.

Figura 1. Ejemplo formato inventario de activos

PROCESO	DUEÑO/RESPONSABLE	CATEGORIA	TIPO	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
GESTION FINANCIERA	CARLOS NEUTO	HARDWARE	SOPORTE	CAJA FUERTE	4	4	4	4
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	IMPRESORAS	3	3	2	2
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	ACCESS POINT	4	4	3	3
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	UPS	4	4	3	4
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE APLICACIONES	4	4	3	4
GESTION LOGISTICA	RAFAEL		SOPORTE	TELEFONO CELULAR	3	3	2	2
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	SISTEMA DE BAKCUP	4	4	4	5
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	DISCO DURO PARA BACKUP	4	4	4	5
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	DVR	4	4	4	4
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	TELEFONOS CELULARES	3	3	2	2
GESTION LOGISTICA	RAFAEL		SOPORTE	CAMIONETA	3	3	2	3
GESTION LOGISTICA	RAFAEL		SOPORTE	MOTO	3	3	2	3
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE ARCHIVOS	4	4	3	4
GESTION FINANCIERA	CARLOS NEUTO		SOPORTE	COMPUTADORES DEL AREA FINANCIERA	3	4	4	3
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	PLANTA TELEFONICA	4	4	3	3
GESTION LOGISTICA	RAFAEL		SOPORTE	COMPUTADORES DEL AREA LOGISTICA	3	4	3	3
GESTION FINANCIERA	CARLOS NEUTO		SOPORTE	TOKEN BANCO	4	5	5	5
GESTION LOGISTICA	RAFAEL		SOPORTE	SISTEMA DE VIGILANCIA	4	4	2	3
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	SWITCHES	4	4	3	3
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	ROUTER	4	4	3	3
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	PARQUE INFORMATICO	4	4	3	3
GESTION FINANCIERA	CARLOS NEUTO	LUGAR	SOPORTE	OFICINAS ADMINISTRATIVAS	4	4	3	3
GESTION LOGISTICA	RAFAEL		SOPORTE	BODEGA DE ALMACENAMIENTO	4	4	4	4
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	CUARTO DE COMUNICACIONES	4	4	4	4
GESTION DE IT	HERIBERTO CEBALLOS		SOPORTE	CUARTO DE SERVICIO TECNICO	4	4	2	3

Fuente: Autor

El listado completo de activos de información se puede encontrar en el anexo C.

4.3.2 Lista de amenazas y vulnerabilidades. La lista de amenazas y vulnerabilidades de cada uno de los activos de información inventariados se determinó con la ayuda de los dueños y responsables de los mismos, pues ellos tienen mayor conocimiento basados en la experiencia del uso diario.

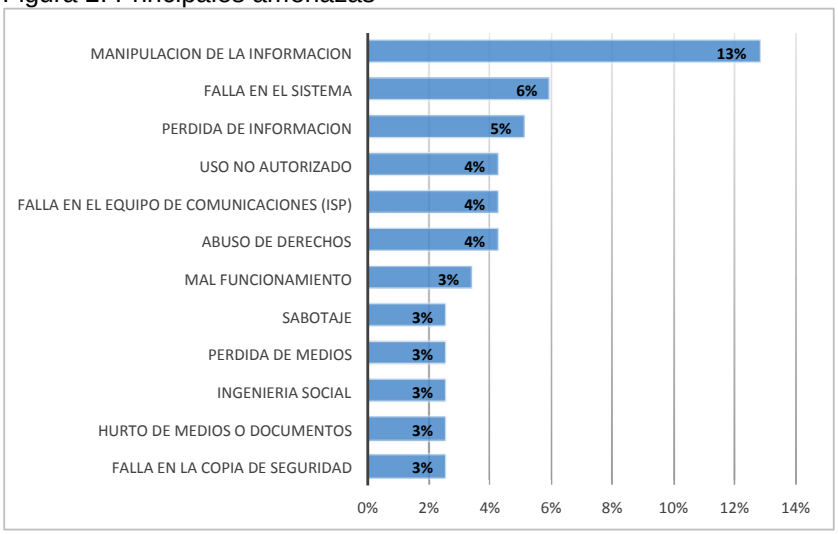
Lista general de amenazas identificadas:

- Abuso de derechos.
- Ausencia y/o no disponibilidad del personal.
- Código malicioso.
- Daño por agua.
- Explotación de configuraciones por defecto.
- Falla en el equipo centralizado de enrutamiento.
- Falla en el equipo de comunicaciones (ISP).
- Falla en el sistema.
- Fallas en el DVR o cámaras.
- Fenómenos climáticos.
- Hurto de información.
- Hurto de medios o documentos.

- Hurto o perdida.
- Incumplimiento de los acuerdos establecidos.
- Ingeniería social.
- Instrucción con credenciales de usuarios retirados.
- Inundación.
- Mal funcionamiento.
- Manipulación con software.
- Manipulación de la información.
- Negación de servicio.
- Perdida de información.
- Perdida de medios.
- Perdida del suministro de energía.
- Polvo o corrosión.
- Procedimiento inadecuado de contratación.
- Procesamiento ilegal de datos.
- Sabotaje.
- Uso inadecuado.
- Uso inadecuado del equipo.
- Uso no autorizado.

La figura 2 presenta las principales amenazas identificadas en Sitech.

Figura 2. Principales amenazas



Fuente: Autor

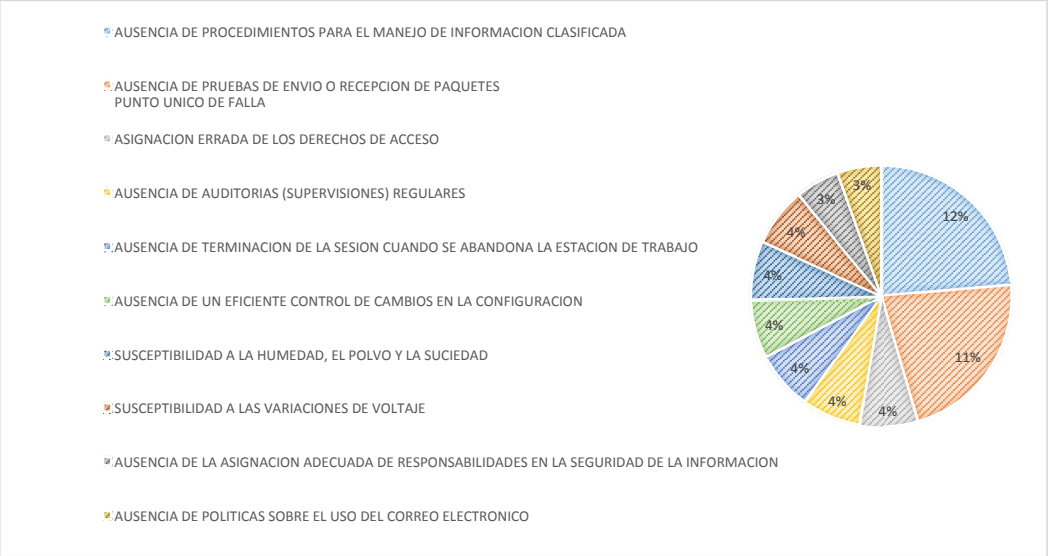
Lista de Vulnerabilidades identificadas:

- Almacenamiento sin protección.
- Ausencia de un eficiente control de cambios en la configuración.
- Copia no controlada.
- Falta de cuidado en la disposición final.
- Falta de seguimiento satelital.
- Habilitación de servicios innecesarios.
- Susceptibilidad a la humedad, el polvo y la suciedad.
- Susceptibilidad a las variaciones de voltaje.

- Ausencia de protección física de la edificación, puertas y ventanas.
- Red energética inestable.
- Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.
- Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos.
- Ausencia de auditorías (supervisiones) regulares.
- Ausencia de la asignación adecuada de responsabilidades en la seguridad de la información.
- Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad.
- Ausencia de planes de continuidad documentados.
- Ausencia de políticas sobre el uso del correo electrónico.
- Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información.
- Ausencia de procedimiento formal para el control de la documentación del SGSI.
- Ausencia de procedimiento formal para el registro y retiro de usuarios.
- Ausencia de procedimiento formal para la autorización de la información disponible al público.
- Ausencia de procedimiento formal para la revisión (supervisión) de los derechos de acceso.
- Ausencia de procedimiento formal para la supervisión del registro del SGSI.
- Ausencia de procedimientos de control de cambios.
- Ausencia de procedimientos de identificación y valoración de riesgos.
- Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.
- Ausencia de procedimientos disciplinarios definidos en el caso de incidentes de seguridad de la información.
- Ausencia de procedimientos para el manejo de información clasificada.
- Ausencia de procedimientos para la introducción del software en los sistemas operativos.
- Ausencia de registros en las bitácoras (logs) de administrador y operario.
- Ausencia de reportes de fallas en los registros de administradores y operadores.
- Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos.
- Ausencia de revisiones regulares por parte de la gerencia.
- Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con clientes o terceras partes.
- Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla.
- Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados.
- Falta de conciencia acerca de la seguridad.
- Entrenamiento insuficiente en seguridad.
- Uso incorrecto de hardware y software.
- Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.
- Procedimiento inadecuado de contratación.
- Ausencia de mecanismos de monitoreo.
- Ausencia de personal.
- Ausencia de pruebas de envió o recepción de paquetes.
- punto único de falla.
- Asignación errada de los derechos de acceso.
- Ausencia de terminación de la sesión cuando se abandona la estación de trabajo.
- Configuración incorrecta de parámetros.
- Descarga y uso no controlado de software.
- Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.
- Falta de actualizaciones requeridas.
- Servicios innecesarios habilitados.

En la figura 3 se puede apreciar el top 10 de vulnerabilidades de Sitech según su porcentaje de ocurrencia en los activos de información.

Figura 3. Top 10 de vulnerabilidades en Sitech



Fuente: Autor

4.3.3 Pruebas de vulnerabilidades. Se realizaron pruebas de vulnerabilidad en aplicaciones web con el uso de la herramienta owasp zap, las cuales se dirigieron a la aplicación de tickets de servicio, el alcance de esta aplicación es tanto para clientes internos, como para contratos de servicio y clientes externos.

Como resultado de las pruebas se pudo identificar 2 alertas de nivel medio y 5 alertas de nivel bajo, las cuales se relacionan a continuación en el cuadro 8.

Cuadro 8. Análisis de vulnerabilidades al software de tickets

Nivel de Riesgo	**Alerta de seguridad**	**Descripción de la alerta**	**Solución recomendada**
Media	*X-Frame-Options Header Not Set*	La cabecera X-*Frame* no tiene configuración	Para evitar ataques de *clickjacking* se recomienda parametrizar la cabecera X-*Frame* con alguna de las opciones valida: *Deny*, para denegar que se muestre la página en un *frame*/*iframe* *Sameorigin*, Solo permite que sea mostrada desde su propio dominio *Allow-From url*, solo permitirá que se muestre desde el *url* señalado
Media	Exploración de Directorios	Es posible ver el listado de directorios, posibilitando el acceso a información sensible a algún atacante	La solución recomendada es desactivar la exploración de directorios, pero en caso de ser necesaria esta funcionalidad, se debe asegurar que el contenido de los directorios que se pueden consultar no contengan información sensible que induce a riesgos
Baja	*Cookie No HttpOnly Flag*	La bandera de *HttpOnly* no está activa	Activar la bandera de HttpOnly para mitigar el riesgo de script del lado del cliente que quiera acceder a la cookie protegida
Baja	*Web Browser XSS Protection Not Enabled*	La cabecera de seguridad para XSS - Cross-*Site* Scripting no está habilitada	Se recomienda activar la cabecera *x-xss-protection* la cual activa el filtro de *corss-site* scripting (XSS) en los navegadores web modernos.

Cuadro 8. (Continuación)

Nivel de Riesgo	Alerta de seguridad	Descripción de la alerta	Solución recomendada
Baja	*Password Autocomplete in Browser*	La función de autocompletar para campos y formularios con contraseñas está habilitado, esto permite que los datos sean almacenados en los navegadores y puedan ser recuperados por atacantes	Desactivar el atributo de autocompletar en formularios entradas para contraseñas
Baja	*X-Content-Type-Options Header Missing*	La cabecera X-Content-*Type-Options* no establece el valor NOSNIFF, el cual mitiga el riesgo de ataque basado en confusión de tipos mime	Asegurarse que en el servidor de aplicaciones web se asigne el valor NOSNIFF a la variable X-Content-Type-*Options* en todas las paginas para evitar que los navegadores que soportan la cabecera carguen hojas de estilo o scripts (*Javascript*) cuyos *Myme*-Type no sea el adecuado. También es importante asegurarse que los usuarios utilizan navegadores actualizados compatibles con los estándares.
Baja	*Private* IP *Disclosure*	Una dirección IP privada se puede encontrar en el cuerpo de las respuestas HTTP, esta información puede ser utilizada por atacantes como objetivo en los sistemas internos.	Se recomienda eliminar la dirección IP privada del cuerpo de respuesta HTTP, Se puede usar JSP/ASP en lugar de los comentarios HTML/Javascript los cuales pueden ser vistos por los navegadores de los clientes.
Fuente: Autor			

El reporte de alertas detallado generado por la herramienta ZAP de owasp se puede consultar en detalle en el Anexo D.

4.3.4 Lista de riesgos de seguridad. Con base en el inventario de activos de información, las vulnerabilidades de cada uno y las amenazas que podrían llegar a explotar estas vulnerabilidades se genera la lista de riesgos de seguridad para le empresa Sitech de Colombia SAS.

Estos se basan en la teoría de la probabilidad de que una amenaza explote una vulnerabilidad de un activo de información generando consecuencias para la organización.

Riesgo = Impacto * Probabilidad de ocurrencia.

En entrevistas con cada uno de los dueños y responsables de los activos de información se calculó el impacto que tendría para la organización la afectación de sus activos, así como la probabilidad de ocurrencia de una amenaza explotando las vulnerabilidades inidentificadas.

Se identificaron un total de 118 activos de información en los procesos de gestión financiera, gestión logística y gestión de IT, los cuales tienen posibles riesgos de seguridad de la información.

Estos riesgos se pueden resumir en los siguientes:

- Falla en los sistemas y hardware.
- Hurto de medios de copias de seguridad.

- Hurto o perdida de dispositivos por falta de seguridad física en las instalaciones.
- Ingeniería social en el personal directo y subcontratado.
- Uso incorrecto de medios de comunicaciones y mensajería.
- Daño en los equipos por factores externos.
- Procesamiento ilegal de datos en archivos y aplicaciones.
- Código malicioso por falta de políticas.

El listado completo de riesgos de seguridad se puede analizar en detalle en el Anexo E.

Cada una de las líneas del listado de riesgos se puede interpretar tal como el siguiente ejemplo: La probabilidad de pérdida y/o hurto de documentos de la caja fuerte debido a que esta se encuentra ubicada en un lugar de almacenamiento sin protección.

En el cuadro 9. se puede evidenciar el formato utilizado en las entrevistas con los dueños y responsables de proceso para identificar los riesgos.

Cuadro 9. Formato de lista de riesgos

Categoría	Tipo (primario - soporte)	Nombre activo	Disponibilidad	Integridad	Confidencialidad	Impacto	Vulnerabilidades	Amenazas
Hardware	Soporte	Caja fuerte	4	4	4	4	Almacenamiento sin protección	Hurto o perdida
	Soporte	Impresoras	3	3	2	2	Almacenamiento sin protección	Manipulación de la información
	Soporte	*Access point*	4	4	3	3	Ausencia de un eficiente control de cambios en la configuración	Explotación de configuraciones por defecto
	Soporte	Ups	4	4	3	4	Ausencia de un eficiente control de cambios en la configuración	Daño por agua
	Soporte	Servidor de aplicaciones	4	4	3	4		Negación de servicio
	Soporte	Teléfono celular	3	3	2	2		Uso inadecuado del equipo
	Soporte	Sistema de *vacuo*	4	4	4	5	Copia no controlada	Falla en el sistema
	Soporte	Disco duro para backup	4	4	4	5		HURTO DE MEDIOS
	Soporte	DVR	4	4	4	4		
	Soporte	Teléfonos celulares	3	3	2	2	Falta de cuidado en la disposición final	Hurto de información
	Soporte	Camioneta	3	3	2	3	Falta de seguimiento satelital	Hurto o perdida por delincuencia en la ciudad
	Soporte	Moto	3	3	2	3		
	Soporte	Servidor de archivos	4	4	3	4	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Soporte	Computadores del área financiera	3	4	4	3	Susceptibilidad a la humedad, el polvo y la suciedad	Falla en el sistema
	Soporte	Planta telefónica	4	4	3	3		MAL FUNCIONAMIENTO
	Soporte	Computadores del área logística	3	4	3	3		PERDIDA DE INFORMACIÓN
	Soporte	*Token* banco	4	5	5	5		UNO NO AUTORIZADO
	Soporte	Sistema de vigilancia	4	4	2	3	Susceptibilidad a las variaciones de voltaje	Polvo o corrosión
	Soporte	Switches	4	4	3	3		
	Soporte	*Router*	4	4	3	3		
	Soporte	Parque informático	4	4	3	3		USO INADECUADO DEL EQUIPO

Fuente: Autor

4.3.5 Evaluación de riesgos (probabilidad/impacto). Tal como el inventario de activos de información, vulnerabilidades y amenazas que se realizó en compañía de los dueños y responsables de los procesos incluidos en el alcance de este proyecto, se realizó la valoración de impacto para la compañía y probabilidad que un activo de información sea afectado por una amenaza.

En total se encontraron 6 riesgos en nivel aceptable, 82 moderados y 30 inaceptables, lo cual se puede evidenciar en el cuadro 10. Resultado de evaluación del riesgo.

Cuadro 10. Resultado de evaluación del riesgo

Nivel de aceptación	Rango de Valores	Cantidad Riesgos
Aceptable	1 - 4	6
Moderado	5 - 9	82
Inaceptable	10 - 25	30
Fuente: Autor		

Fuente: Autor

El resultado se puede examinar en detalle en el anexo F, sin embargo a continuación en la figura 4 se presenta un ejemplo del formato utilizado para valorar el impacto y la probabilidad de ocurrencia.

Figura 4. Formato valoración de impacto y probabilidad.

PROCESO	SUBPROCESO	DUEÑO /RESPONSABLE	CATEGORIA	TIPO (PRIMARIO - SOPORTE)	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO	VULNERABILIDADES	AMENAZAS	PROBABILIDAD DE OCURRENCIA	RIESGO
GESTION FINANCIERA	CONTABILIDAD	CARLOS NEUTO	HARDWARE	SOPORTE	CAJA FUERTE	4	4	4	4	ALMACENAMIENTO SIN PROTECCION	HURTO O PERDIDA	2	8
GESTION DE IT	INFRAESTRUCTURA	HERIBERTO CEBALLOS		SOPORTE	IMPRESORAS	3	3	2	2	ALMACENAMIENTO SIN PROTECCION	MANIPULACION DE LA INFORMACION	4	8
GESTION DE IT	INFRAESTRUCTURA	HERIBERTO CEBALLOS		SOPORTE	ACCESS POINT	4	4	3	3	AUSENCIA DE UN EFICIENTE CONTROL DE CAMBIOS EN LA CONFIGURACION	EXPLOTACION DE CONFIGURACIONES POR DEFECTO	3	9
GESTION DE IT	INFRAESTRUCTURA	HERIBERTO CEBALLOS		SOPORTE	UPS	4	4	3	4	AREA FISICA NO SEGURA	DAÑO POR AGUA	3	12
GESTION DE IT	INFRAESTRUCTURA	HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE APLICACIONES	4	4	3	4		NEGACION DEL SERVICIO	2	8
GESTION LOGISTICA	LOGISTICA	RAFAEL		SOPORTE	TELEFONO CELULAR	3	3	2	2	AUSENCIA DE UN EFICIENTE CONTROL DE CAMBIOS EN LA CONFIGURACION	USO INADECUADO DEL EQUIPO	4	8
GESTION DE IT	INFRAESTRUCTURA	HERIBERTO CEBALLOS		SOPORTE	SISTEMA DE BAKCUP	4	4	4	5		FALLA EN EL SISTEMA	3	15

Fuente: Autor

4.3.6 Lista de riesgos priorizados. Esta lista se basa en el peso de cada riesgo lo cual indica que tiene mayor probabilidad de ocurrencia e impacto para la organización en caso de ser afectado por una amenaza.

Este es el top de los riesgos con mayor impacto y probabilidad de ocurrencia en la empresa y sobre los cuales se debe tomar acción para evitar impactos negativos:

- Falla en el sistema de copias de seguridad debido a falta de controles y pruebas de resultado.
- Hurto o pérdida del Disco Duro de *backup* externo por falta de control o copia no controlada.
- Copia no controlada en grabaciones del sistema DVR del circuito cerrado de vigilancia.
- Hurto o pérdida de equipos o medios en el cuarto de comunicaciones debido a falta de seguridad física en la habitación.
- Manipulación de la información de contratos de servicio por falta de controles y verificación.
- Falla en los servicios u operación por ausencia de planes de continuidad de negocio.
- Ingeniería social en el personal de la compañía por falta de entrenamiento y conciencia en seguridad de la información.
- Exposición indebida de información debido a la ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.
- Abuso de derechos por parte del personal directo y subcontratado por procedimientos inadecuados en la contratación.
- Ausencia y/o no disponibilidad de personal para la ejecución de servicios subcontratados.

El cuadro 11 muestra la lista completa de riesgos priorizados para Sitech de Colombia SAS.

Cuadro 11. Lista de riesgos priorizados

Categoría	Tipo (primario - soporte)	Nombre activo	Disponibilidad	Integridad	Confidencialidad	Impacto	Vulnerabilidades	Amenazas	Probabilidad de ocurrencia	Riesgo
Hardware	Soporte	Ups	4	4	3	4	Ausencia de un eficiente control de cambios en la configuración	Daño por agua	3	12
	Soporte	Sistema de *bakcup*	4	4	4	5	Copia no controlada	Falla en el sistema	3	15
	Soporte	Disco duro para backup	4	4	4	5			4	20
	Soporte	DVR	4	4	4	4		HURTO DE MEDIOS	4	16
	Soporte	Servidor de archivos	4	4	3	4	Habilitación de servicios innecesarios	Procesamiento ilegal de datos	3	12
	Soporte	Planta telefónica	4	4	3	3	Susceptibilidad a la humedad, el polvo y la suciedad	Mal funcionamiento	4	12
	Soporte	*Token* banco	4	5	5	5		UNO NO AUTORIZADO	2	10
	Soporte	Sistema de vigilancia	4	4	2	3	Susceptibilidad a las variaciones de voltaje	Polvo o corrosión	4	12
	Soporte	*Switches*	4	4	3	3			4	12
	Soporte	*Router*	4	4	3	3			4	12
Lugar	Soporte	Bodega de almacenamiento	4	4	4	4	Ausencia de protección física de la edificación, puertas y ventanas	Inundación	3	12
	Soporte	Cuarto de comunicaciones	4	4	4	4		HURTO	4	16
Organización	Primario	Contratos de servicios	4	4	4	5	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Manipulación de la información	3	15
	Primario	Pago a proveedores	4	4	4	5	Ausencia de auditorías (supervisiones) regulares	Abuso de derechos	2	10
	Primario	Continuidad de negocio	4	5	5	5	Ausencia de planes de continuidad documentados	Negación de servicio	3	15
	Primario	Creación de credenciales (ad, correo, ERP)	3	3	4	3	Ausencia de procedimiento formal para el registro y retiro de usuarios	Instrucción con credenciales de usuarios retirados	4	12
	Primario	Factura de cliente	3	4	2	3	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Perdida de medios	4	12
	Primario	Comprobantes de recibo de mercancía	2	4	3	4	Ausencia de procedimientos para el manejo de información clasificada		3	12
	Primario	Información financiera de clientes	3	4	5	4	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Uso no autorizado	3	12
	Primario	Planilla de recorrido diario - ruta	3	3	3	4	Ausencia de registros en las bitácoras (*logs*) de administrador y operario	Error en el uso	3	12
Persona	Primario	Empleados	4	4	4	5	Falta de conciencia acerca de la seguridad	Ingeniería social	4	20
	Soporte	Personal de mensajería	4	4	3	5	Entrenamiento insuficiente en seguridad	Ingeniería social	4	20
	Soporte	Ingenieros de soporte	4	4	3	5	Uso incorrecto de hardware y software	Ingeniería social	3	15
	Soporte	Ingenieros de soporte	4	4	3	5	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Perdida de información	3	15
	Soporte	Personal de *outsourcing* técnico	4	4	3	5	Procedimiento inadecuado de contratación	Abuso de derechos	3	15
	Soporte	Personal de outsourcing técnico	4	4	3	5	Ausencia de mecanismos de monitoreo	Destrucción de equipos o medios	2	10
	Soporte	Personal de outsourcing técnico	4	4	3	5	Ausencia de personal	Ausencia y/o no disponibilidad del personal	3	15
Red	Soporte	Red de energía regulada	4	4	2	4	Ausencia de pruebas de envió o recepción de paquetes punto único de falla	Mal funcionamiento	3	12
Software	Primario	Base de datos de clientes	3	4	4	4	Configuración incorrecta de parámetros	Manipulación con software	3	12
	Soporte	Servidor virtual de tickets	4	4	3	3	Descarga y uso no controlado de software	Código malicioso	4	12

Fuente: Autor

4.3.7 Declaración de aplicabilidad. La declaración de aplicabilidad se desarrolló de acuerdo al alcance de los procesos de Sitech de Colombia SA, en conjunto con la alta dirección se determinó de los controles del anexo A de la norma ISO 27001:2013 cuales aplican y cuáles no, justificando la razón de porque no aplican o se tomaran en cuenta.

En resumen los controles que no aplican para Sitech de Colombia son:

A.10.1.1 Política en el uso de controles criptográficos.
A.10.1.2 Gestión de llaves.
A.14.2.1 Política de desarrollo seguro.
A.14.2.2 Procedimientos de control de cambios en sistemas.
A.14.2.6 Ambiente de desarrollo seguro.
A.14.2.8 Pruebas de seguridad de sistemas.

Adicional según la declaración de aplicabilidad se pudo identificar que aunque Sitech no tiene un SGSI implementado se cumple en la actualidad con 27 controles de la norma ISO 27001:2013.

El resultado de la declaración de aplicabilidad se puede consultar en detalle en el Anexo G.

4.3.8 Plan de tratamiento de riesgos. Los planes de tratamiento de riesgos surgen del agrupamiento de los mismos, se identificaron cuales riesgos comparten amenazas y vulnerabilidades que pueden ser tratados con los mismos controles, siendo conscientes que un control puede servir para más de un riesgo.

En resumen la mayoría de los riesgos pueden ser tratados con la implementación de políticas y la concientización del personal de la compañía.

4.3.8.1 Plan de tratamiento para la manipulación de información. El riesgo de manipulación no autorizada de la información se presenta en varios de los activos de información, debido principalmente a la falta de procedimientos definidos y controles de verificación periódicos.

Los riesgos de manipulación de información asociados a este plan se presentan en:

- Acceso a información impresa clasificada en las bandejas de las impresoras.
- Alteración de la información en los contratos de servicio.
- Alteración de la información de terceros aprovechando el proceso de verificación de datos
- Creación de cuentas contables, gestión de cuentas por pagar, comprobantes de causación..
- Formatos y proceso de legalización de gastos, anticipos, cuentas por pagar.
- Informes financieros, extracto bancarios, conciliaciones bancarias, parafiscales.
- Registros de proveedores, de aportes parafiscales.
- Código fuente de sistemas o desarrollos.
- Inventario de activos tecnológicos y sistemas de información.

Tipo de Tratamiento: El tipo de tratamiento seleccionado para este plan es la reducción.

La descripción detallada del tratamiento a realizar se lista a continuación:

- Implementar el servicio de control de impresión segura.
- Definir un plan de seguimiento a los contratos de servicio y sus acuerdos de nivel de servicio en un documento formal.
- Diseñar e implementar un procedimiento de revisión de eventos en la actividad de verificación de datos de terceros.
- Implementar un procedimiento formal para el control de documentación.
- Implementar un procedimiento formal para la autorización de la información disponible al público.
- Asignación adecuada de responsabilidades en la seguridad de la información.
- Implementar un procedimiento formal para la revisión de los derechos de acceso.
- Implementar un procedimiento de manejo de información clasificada.

- Realizar revisiones periódicas por la alta gerencia de los procesos.
- Incluir disposiciones de seguridad de la información en los contratos de los empleados.
- Implementar un procedimiento de identificación y valoración de riesgos.
- Definir e implementar un control en la gestión de garantías.

El resultado esperado con este plan de tratamiento de riesgos es reducir la probabilidad de ocurrencia de la manipulación de información en procesos, documentos físicos en beneficio propio de los empleados o de terceros.

Los controles de la norma ISO 27001:2013 a implementar son los siguientes:

- A.6.1.1
- A.7.1.2
- A.7.2.1
- A.8.2.2
- A.8.2.3
- A.9.2.5
- A.9.4.2
- A.12.1.1
- A.12.4.1
- A.13.2.4
- A.15.2.1
- A.18.1.3
- A.18.2.2

Los responsables de este plan de tratamiento de riesgos son el Gerente de IT, Jefe de logística, jefe financiero.

4.3.8.2 Plan de tratamiento para el abuso de derechos y procesamiento ilegal de datos. El riesgo de abuso de derechos y procesamiento ilegal de datos se presentan principalmente por la falta de procedimientos definidos y ausencia de controles periódicos.

Estos riesgos se identificaron en alguna de las siguientes actividades o activos:

- Gestión de garantías.
- Pago a proveedores.
- Realización de consignaciones.
- Custodia de bienes.
- Servidor de archivo.
- Estados financieros.
- Impuestos.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Diseñar e implementar el procedimiento de gestión de garantías.
- Diseñar e implementar el procedimiento de pago a proveedores.
- Diseñar e implementar el procedimiento de identificación y valoración de riesgos en activos.
- Definir e implementar un control periódico para validar el cumplimiento del procedimiento de realización de consignaciones, pago a proveedores, estados financieros e impuestos.

- Definir e implementar un procedimiento para la apertura o activación de servicios estrictamente necesarios.

El resultado esperado con el plan de tratamiento es evitar el abuso de derechos y el procesamiento ilegal de datos al definir los pasos a seguir en la ejecución de actividades realizando verificaciones periódicas para supervisar cumplimientos.

Los controles de la norma ISO 27001:2013 a implementar son los siguientes:

- A.9.1.2
- A.12.4.1
- A.12.1.1
- A.18.2.3

Los responsables de este plan de tratamiento de riesgos son el jefe de logística, jefe financiero y gerente de IT.

4.3.8.3 Plan de tratamiento para el uso no autorizado/adecuado de activos de información. El riesgo de uso no autorizado o inadecuado de activos de información se presenta principalmente por la ausencia de procedimientos y controles para aumentar la protección física y lógica.

Estos riesgos se identificaron en actividades, hardware o software como se muestra a continuación:

- Parque de teléfonos celulares.
- *Tocken* bancario.
- Parque informático.
- Informes del área logística.
- Comprobantes de nómina.
- Diagrama de red.
- Información financiera de Clientes.
- Planilla de recorrido diario – ruta.
- Inventario de Vehículos.
- Directorio telefónico de clientes y proveedores.
- ERP *WorldOffice.*
- Software de tickets.
- Consola de antivirus.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Implementación de políticas para el uso adecuado de dispositivos móviles incluyendo teléfonos celulares, tabletas, portátiles y demás recursos tecnológicos que permitan el procesamiento de información.
- Se deben tomar las medidas necesarias para que las oficinas, principalmente las del área financiera y tesorería sean seguras, evitando robos o pérdida de dispositivos o documentos.
- Implementar un procedimiento específico para el manejo adecuado de los activos de información.
- Diseñar un procedimiento que especifique la presentación correcta de informes y su correcta custodia para evitar a perdida de información.

- Asignar adecuadamente las responsabilidades en la seguridad de la información, asegurándose desde el momento de la contratación que todos los empleados conozcan su papel en la seguridad y las implicaciones del no cumplimiento.
- Diseñar un procedimiento para el correcto majeño de la información clasificada.
- Diseñar e implementar un control periódico de los registros, bitácoras o logs tanto de los sistemas como de las actividades de los empleados que así lo ameriten.
- Implementar procedimientos de control de cambios en los sistemas.
- Definir un plan de pruebas para todo cambio realizado en los sistemas de información o implementaciones nuevas.

El resultado esperado con este plan de tratamiento es disminuir la probabilidad de ocurrencia de uso no adecuado/autorizado en los activos de información.

Los controles de la norma ISO 27001:2013 a implementar son los siguientes:

- A.6.1.1
- A.6.2.1
- A.7.1.2
- A.7.2.2
- A.8.1.3
- A.8.2.1
- A.8.2.3
- A.9.1.1
- A.9.2.1
- A.9.2.3
- A.9.2.5
- A.11.1.1
- A.11.1.3
- A.12.1.2
- A.12.4.1
- A.12.4.2
- A.12.4.3
- A.13.2.4
- A.14.2.4
- A.14.2.5

Los responsables de este plan de tratamiento de riesgos son el jefe de logística, jefe financiero y gerente de IT.

4.3.8.4 Plan de tratamiento para perdida o hurto de medios o información. El riesgo de pérdida o hurto de información o medios se presenta principalmente por la falta de definiciones de responsabilidades de seguridad de la información para el personal de Sitech, así como la ausencia de controles y procedimientos específicos que ayuden a mitigar la probabilidad de ocurrencia de este riesgo.

Se identificó la probabilidad de ocurrencia de este riesgo en los siguientes activos de información:

- Caja Fuerte.
- Disco Duro para copias de seguridad.
- Disposición de teléfonos celulares.
- Computadores del área logística.
- Documentación de garantías.

- Informes de revisoría fiscal.
- Manuales de usuario.
- Plano del edificio.
- Facturas de clientes.
- Comprobantes de devolución de mercancía.
- Documentos para el estudio de crédito.
- Contratos.
- Backup de archivos gestión financiera.
- Carpeta compartida del área financiera.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Implementar medidas de seguridad adecuadas para la protección de los activos en las oficinas del área financiera, incluyendo medias especiales para el uso de la caja fuerte.
- Diseñar e implementar procedimiento de ejecución, verificación y custodia de copias de seguridad.
- Diseñar e implementar un procedimiento formal para la disposición de activos de procesamiento información.
- Implementar un control de seguimiento satelital a los vehículos de la compañía.
- Establecer mecanismos de monitoreo para las brechas de seguridad.
- Definir un procedimiento formal para la autorización de información disponible al público.
- Diseñar e implementar procedimientos de gestión de cambios.
- Implementar procedimientos de manejo de información clasificada.
- Diseñar e implementar una política de escritorio limpio y pantalla limpia.
- Diseñar e implementar un control de pruebas de envío y recepción de paquetes en la red.

El resultado esperado con este plan de tratamiento es disminuir la probabilidad de hurto o pérdida de información o medios en las instalaciones de Sitech de Colombia SAS.

Los controles de la norma ISO 27001:2013 a implementar son:

- A.8.2.1
- A.8.2.3
- A.8.3.2
- A.11.1.1
- A.11.1.3
- A.11.1.4
- A.11.2.6
- A.11.2.7
- A.11.2.9
- A.12.3.1
- A.13.2.1
- A.18.1.2

Los responsables de la implementación de este plan de tratamiento de riesgos son el jefe financiero, jefe de logística y gerente de IT.

4.3.8.5 Plan de tratamiento para la falla en los equipos/sistemas. El riesgo de fallas en los equipos o sistemas se presenta principalmente por ausencia de pruebas y controles en los puntos

únicos de falla, controles eficientes de cambios y configuraciones y las condiciones ambientales que no se tienen en cuenta.

Se identificó la probabilidad de ocurrencia de este riesgo en los siguientes activos de información:

- Los servicios provistos por terceros tales como la telefonía, internet y aplicaciones que se soporten sobre los mismos, que tienen sus equipos centralizados en el cuarto de comunicaciones.
- Los servicios o aplicaciones propias de la compañía tales como el ERP, red de datos, dominio y demás herramientas centralizadas en el cuarto de comunicaciones.
- Aplicaciones cliente en cada uno de los equipos del parque informático.
- Sistema de copias de seguridad.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Diseñar e implementar un eficiente sistema de control de cambios en las configuraciones de los equipos centralizados.
- Establecer una política de pruebas periódicas en los puntos centralizados de procesamiento o enrutamiento de información.
- Diseña e implementar un procedimiento de gestión de accesos junto con una política de verificación periódica de la vigencia de las asignaciones de privilegios.
- Implementar un control específico para los cambios en configuraciones y parámetros la cual debe ser debe ser validada con periodicidad.
- Diseñar e implementar una policita para la correcta disposición y/o reutilización de medios de almacenamiento de información.

El resultado esperado con este tratamiento es disminuir la probabilidad de fallas en los equipos o sistemas por configuraciones por defecto, falta de control de cambios o condiciones físicas y ambientales.

Los controles de la norma ISO 27001:2013 a implementar son:

- A.8.3.2
- A.9.2.1
- A.9.2.2
- A.9.2.6
- A.11.1.4
- A.11.2.1
- A.11.2.7
- A.12.1.2
- A.13.2.1
- A.14.2.2
- A.14.2.4

Los responsables de la implementación de este plan de tratamiento de riesgos son el gerente de IT, jefe financiero, jefe de logística y Auxiliar contable.

4.3.8.6 Plan de tratamiento para riesgos relacionados con sabotaje y el personal. Los riesgos de seguridad de la información relacionados con sabotaje y el personal en Sitech de Colombia se

presentan principalmente por falta de conciencia en seguridad, controles eficientes y procedimientos definidos y socializados al personal.

Se identificó la probabilidad de ocurrencia de riesgos relacionados con personal en los siguientes activos de información:

- Documentación de remisiones.
- Indicadores de medición.
- Personal de Outsourcing técnico.
- Ingenieros de soporte.
- Personal de mensajería y empleados en general.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Diseñar e implementar un procedimiento y política de concienciación del personal en temas de seguridad de la información.
- Implementar un procedimiento adecuado para la contratación de personal, donde se realicen las verificaciones mininas de seguridad.
- Diseñar una policita donde se contemplen mecanismos de monitoreo a las actividades del personal con el fin de evitar los riesgos ocasionados por ingeniería social.
- Los procedimientos para el control de cambios y manejo de información clasificada plantean en los tratamientos de riesgos anteriores.
- Diseñar, implementar y socializar una política de buenas prácticas para la gestión de contraseñas.

El resultado esperado con este tratamiento es disminuir la probabilidad de sabotaje de documentos por parte del personal de Sitech, o el aprovechamiento de la falta de conocimiento en seguridad de la información o los procedimientos internos de la compañía.

Los controles de la norma ISO 27001:2013 a implementar son:

- A.6.1.1
- A.7.1.1
- A.7.1.2
- A.7.2.2
- A.7.2.3
- A.8.2.1
- A.9.3.1

Los responsables de la implementación de este plan de tratamiento de riesgos son el gerente de IT, Jefe de logística, feje financiero, auxiliar contable y el jefe de recursos humanos.

4.3.8.7 Plan de tratamiento para amenazas informáticas. Los riesgos de seguridad asociados a amenazas informáticas están relacionados principalmente a la falta de procedimientos y políticas de ejecución y verificación en los diferentes sistemas, listas de chequeo para evitar configuraciones por defecto o controles en los cambios se encuentran en los primeros lugares de las vulnerabilidades de para estos riesgos.

Se identificó la probabilidad de ocurrencia de riesgos relacionados con amenazas informáticas en los siguientes activos de información:

- Puntos de acceso inalámbrico.
- Servidores de aplicaciones y archivos, tanto físicos como virtuales.
- Bases de datos en aplicaciones
- Actividad de gestión de credenciales.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Diseñar e implementar procedimientos y controles eficientes para la gestión de cambios en configuraciones de equipos de comunicación, servidores y aplicaciones.
- Diseñar e implementar una política y procedimiento de plan de continuidad del negocio, la cual se ponga a prueba por lo menos una vez cada año.
- Diseñar e implementar un procedimiento formal de gestión de credenciales de acceso, realizando el debido proceso de baja al momento de retiro de un colaborador de la compañía.
- Implementar una política de verificación periódica de cuentas activas en las diferentes aplicaciones y servicios.
- Implementar una política de ejecución de actualizaciones de seguridad y generales en cada uno de los sistemas de la compañía, incluyendo firmware de dispositivos.
- Diseñar e implementar procedimientos para controlar la instalación de software en sistemas operativos.
- Diseñar e implementar políticas y controles para la verificación de servicios activos innecesarios en los sistemas.
- Diseñar e implementar un procedimiento y política de copias de seguridad de los sistemas de información, configuraciones y firmware de los dispositivos periódicamente.

El resultado esperado con este tratamiento es disminuir la probabilidad de afectaciones en Sitech de Colombia debidas a explotación de amenaza informáticas en los diferentes sistemas de la compañía.

Los controles de la norma ISO 27001:2013 a implementar son:

- A.9.2.2
- A.9.2.3
- A.9.2.5
- A.9.2.6
- A.12.1.2
- A.12.2.1
- A.12.3.1
- A.13.1.2
- A.13.2.1
- A.14.2.2
- A.14.2.4
- A.17.1.1
- A.17.1.2
- A.17.1.3

Los responsables de la implementación de este plan de tratamiento de riesgos son el gerente de IT, jefe financiero y jefe de logística.

4.3.8.8 Plan de tratamiento para fenómenos climáticos, ambientales o servicios. Los riesgos de seguridad relacionados con condiciones ambientales o fenómenos climáticos son difíciles y más complicados de prevenir, pero se pueden tratar para disminuir sus efectos.

Los activos de información que se pueden ver afectados por estos riesgos se identificaron para Sitech de Colombia y se exponen en la siguiente lista:

- Equipos y dispositivos en el cuarto de comunicaciones.
- Bodega de almacenamiento.
- Instalaciones de la empresa en general.
- Sistema cerrado de vigilancia.

El tipo de tratamiento a implementar es reducción.

La descripción detallada del tratamiento a implementar es:

- Diseñar e implementar controles de acceso y seguridad físicos en áreas de procesamiento de datos.
- Diseñar e implementar controles para las variaciones de voltaje en la red.
- Diseñas e implementar controles de seguridad física en oficinas, recintos e instalaciones.
- Diseñar e implementar controles sobre los puntos de acceso de mercancía y áreas de despacho.

El resultado esperado con este tratamiento es disminuir el impacto de afectaciones en Sitech de Colombia debidas a condiciones ambientales anormales y fenómenos climáticos.

Los controles de la norma ISO 27001:2013 a implementar son:

- A.11.1.1
- A.11.1.2
- A.11.1.3
- A.11.1.4
- A.11.1.5
- A.11.2.3

Los responsables de la implementación de este plan de tratamiento de riesgos son el gerente de IT y el jefe de logística.

4.3.9 Principales políticas de seguridad a adoptar. El uso de políticas de seguridad permite a Sitech de Colombia SA comunicarse con las partes interesadas, estableciendo un canal para definir la forma de actuar en relación con los recursos y servicios informáticos de la seguridad de la información.

A continuación se describen algunas recomendaciones de políticas de seguridad de la información para adoptar en Sitech.

4.3.9.1 Política de formación en competencias y conciencia de la seguridad.

Objetivo: Establecer una conciencia de seguridad y programa de entrenamiento que explique las reglas apropiadas de comportamiento para la seguridad de la información eficaz. El programa comunica políticas de seguridad, procedimientos y competencias que deben seguirse, y sienta las bases para las medidas disciplinarias necesarias debido a la falta de cumplimiento.

Alcance: Esta política se aplica a todos los empleados, contratistas y terceros en base a su relevancia para cada función de trabajo, a los usuarios del sistema de información, y a los propietarios con activos identificados dentro del Sistema de Gestión de Seguridad de Sitech de Colombia SA.

Definiciones:

SGSI. Sistema de Gestión de Seguridad de la Información, es la parte del sistema general de gestión, basado en un enfoque de riesgo empresarial, que establece, implementa, opera, monitorea, mantiene y mejora la seguridad de la información.

ESGSI. Equipo del sistema de Gestión de Seguridad de la Información, son los empleados cuyas funciones los define como recurso dedicado a la implantación y mantenimiento del SGSI.

Trabajadores. Se refiere a todos los empleados y trabajadores eventuales, ayuda temporal, contratistas, consultores, etc.

Roles:

Toda la administración: Responsables de:

Asegura que todos los nuevos trabajadores sean capacitados en el cumplimiento del SGSI dentro del tiempo permitido a partir de la fecha de contratación.

Garantizar que los trabajadores que realizan trabajos que afectan al SGSI estén capacitados y competentes.

Garantizar la conservación de los registros de formación en seguridad de la información como evidencia de la competencia.

Todos los empleados:

Completar todos los entrenamientos de Seguridad de la información de Manera Oportuna.

Leer, comprender y adherirse a las condiciones generales del SGSI incluyendo, pero no limitándose a: la seguridad física, escritorio limpio/pantalla limpia, uso de la contraseña segura y la protección de los activos.

Política:

Todos los usuarios de los sistemas de información, independientemente de su cargo laboral, deben asistir a la formación de la conciencia en seguridad de información (en línea o en persona) cada año. Este material debe proporcionar los fundamentos de seguridad de la información y la alfabetización.

Todos los trabajadores deben contar con la suficiente formación y el material de apoyo de referencia que les permita proteger adecuadamente los recursos de información de Sitech. El equipo de SGSI debe coordinar con TI, la gestión operativa para proporcionar la formación necesaria a los empleados para cumplir con el SGSI y la concienciación sobre la seguridad en general. Todos los empleados deben recibir formación general relacionada con la información y la seguridad física de su trabajo a través de herramientas *e-learning* (on-line) o en persona, por sus supervisores inmediatos, o por un entrenador calificado. El material debe contener información formal, debe ser comunicado, en lugar de tomar medidas contra los trabajadores que han cometido una violación de la seguridad de la información.

Todo trabajador, independientemente de la clasificación profesional, debe asistir a una clase de conciencia de seguridad de la información dentro de un tiempo razonable después de haber comenzado labores con Sitech. Si el entrenamiento se entrega a través de *e-learning*, se debe generar una prueba de competencia o el reconocimiento y aceptación por parte del trabajador.

Todo el personal que participa activamente y tiene responsabilidades en el SGSI debe tener o se le debe proporcionar entrenamiento formal.

Se debe definir un tiempo suficiente para que los trabajadores se familiaricen con las políticas de seguridad, procedimientos de Sitech, y las labores de la empresa.

Además cada jefe debe asegurarse de que sus subordinados directos tienen la suficiente formación y conocimientos técnicos para poder operar con seguridad los sistemas de información de Sitech.

Programa de Capacitación

Formación en seguridad de la información y plan de sensibilización:
La alta dirección de Sitech debe desarrollas y documentar un plan para la sensibilización en seguridad de la información, formación y educación de toda la organización.

Responsabilidad de entrenamiento:
El equipo del SGSI deberá proporcionar el apoyo adecuado a la educación y formación por medio de canales de comunicación predefinidos. Así como revisar y aprobar toda la información relacionada con seguridad de la información la cual debe ser coherente.

Cualificación de los formadores: Los entrenadores internos deben estar cualificados en base a la educación y/o experiencia relacionada con el trabajo y deben ser seleccionados por el manejo responsable de cada área. Si se subcontratan capacitadores, estos deben estar acreditados por una organización reconocida, estos deben cumplir con toda las políticas de Sitech para asegurar que todos los activos de información estarán protegidos.

Especificaciones mínimas de la formación de seguridad de la información: Se debe especificar un conjunto mínimo de requisitos de formación y sensibilización para todos los trabajadores que tienen acceso a la información de Sitech.

Evaluación periódica de la concienciación:

Los métodos para evaluar la efectividad del entrenamiento pueden variar en función de la finalidad. Algunas de las técnicas de evaluación pueden incluir cualquiera de los siguientes:

- Durante el trabajo - Observación por el supervisor el trabajo.
- Efectividad de cursos de formación –Encuestas o evaluaciones para validar la efectividad de los diversos métodos utilizado para promover conciencia incluyendo los cursos *e-learning*.
- Promover la verificación de la eficacia de la formación se puede hacer durante las auditorías internas.

Registro de Información de Capacitación en Seguridad: Sitech debe mantener un registro de cada trabajador que asiste a una clase de entrenamiento de seguridad de la información. Como mínimo, el registro de entrenamiento debe incluir el nombre del empleado, puesto de trabajo, departamento, fecha de la formación y el tipo de entrenamiento.

Si el entrenamiento es virtual (*e-learning*) el resultado de estos entrenamientos deberán ser capturados electrónicamente y almacenados en el historial de formación de cada empleado. Para los casos de proveedores o terceros que no tengan acceso al sistema de *e-learning* de Sitech, los métodos manuales deberán ser empleados para capturar y preservar la efectividad de la formación en seguridad de la información.

Programa de formación de auditor SGSI

Requisitos para auditores internos SGSI.

- Debe tener una certificación valida de auditor interno ISO 27001:2013.
- 3 años o más de experiencia trabajando en auditoría.
- Debe ser discreto, sentido de juicio, capacidad analítica, tenacidad, capacidad de percibir las situaciones reales.
- Debe tener capacidad de comunicarse eficazmente.

Requisitos de formación.

Auditor Interno de seguridad de la información: Las personas que reúnan los requisitos y sean recomendados por el director SGSI o su superior.

Auditor líder de seguridad de la información: Aquellos auditores Internos SGSI que hayan completado un mínimo de 20 horas o 4 auditorías dentro de los últimos tres (3) años y que han sido recomendados por el director SGSI.

Versión	Fecha	Origen
1	31/07/10	Equipo SGSI

4.3.9.2 Política de escritorio limpio y pantalla limpia.

Objetivo: Esta política establece directrices y establece las expectativas de la conciencia y las prácticas de seguridad de los empleados con el fin de proteger la información confidencial de Sitech de Colombia S.A.

Alcance: Esta política se aplica a todos los empleados de Sitech.

Definiciones:

Información confidencial: Cualquier información de Sitech que no se conoce públicamente e incluye información tangible e intangible en todas sus formas, información que se observa de forma oral, o está en forma electrónica o escrita o en otra forma tangible. Esta definición incluye información marcada como restringido o de uso interno. Información confidencial puede incluir, pero no se limitan a, código fuente, los diseños de productos, resultados de benchmarking, solicitudes de patentes, métodos de producción, hojas de ruta de productos, listas e información de clientes, listas e información de clientes potenciales, planes de promoción, información sobre la competencia, nombres, salarios, habilidades, posiciones, resultados financieros pre-públicos, costos de productos y precios, la información de los empleados incluyendo organigramas.

Roles: Todos los empleados directos de Sitech, trabajadores temporales y Contratistas.

Política:

Protección de la información sensible.

Todos los empleados de Sitech que manejan información confidencial de la empresa deben ocultar adecuadamente esta información de su divulgación no autorizada a partes no autorizadas en las inmediaciones. Esta información confidencial puede ser en forma de documentos originales, copias de originales, documentos electrónicos / archivos e incluso conversaciones verbales.

Los activos de información deben ser manejados con gran cuidado para evitar que las personas que no están autorizados consigan acceso a estos activos de información.

Los documentos que contengan información confidencial o sensible deben ser retirados de las impresoras inmediatamente.

Las pantallas de los ordenadores utilizados para manejar información confidencial deben ser colocadas de tal manera que las personas no autorizadas no puedan ver con facilidad sobre el hombro de la persona que utiliza el computador. Las pantallas deben estar colocados de tal manera que la información sensible no se puede ver a través de ventanas o tragaluces utilizando binoculares o telescopios.

El acceso a todas las oficinas, sala de cómputo y áreas de trabajo que contiene información confidencial debe ser asegurado adecuadamente.

Los gerentes o supervisores deben revisar las áreas de los trabajadores periódicamente para asegurar que la información confidencial no está en riesgo. Es la responsabilidad de los gerentes o supervisores para asegurar la conformidad con la política de escritorio limpio y pantalla limpia, todo material confidencial que se encuentre expuesto, deberá tomarlo en custodia. Se debe tomar como practica una verificación de información confidencial expuesta al finalizar el día laboral.

Horas no laborales.

Todos los empleados deben limpiar sus escritorios y áreas de trabajo de tal manera que toda la información confidencial esté bien asegurada.

Los escritorios deben estar limpios durante las horas no laborales con toda la información confidencial protegida y/o bajo llave.

Todos los equipos, excepto equipos independientes situados en zonas con estrictos controles de acceso físico, que han sido utilizados para el procesamiento de la información confidencial deben ser bloqueados o apagados al finalizar del día.

Uso activos durante las horas de trabajo

A menos que la información confidencial este en uso por personal autorizado, esta debe estar bien protegida y/o almacenada. La información confidencial debe estar ocultada a personal no autorizadas.

La información confidencial en forma impresa debe estar asegurada cuando no esté en uso activo, incluso si está dentro de un edificio cuyo acceso está controlado. Si no está cifrada, toda la información confidencial debe ser protegida en cajas fuertes, muebles pesados, u otros recipientes.

Cada vez que un empleado de Sitech se retire de su equipo de cómputo, este debe bloquear la pantalla para evitar el acceso no autorizado. El ajuste de activación del protector de pantalla se debe programar adecuadamente para el entorno de trabajo de los usuarios. Al dejar desatendida una pantalla.

Los empleados nunca deben escribir sus contraseñas en presencia de personas que puedan observarlos al momento de digitar.

Oficinas y salas de reuniones vacías.

Si existe información confidencial en una oficina sin vigilancia, esta debe ser protegida cerrando la oficina con seguridad, y/o en un archivador, un cajón del escritorio, muebles de seguridad o en otro contenedor con un mecanismo de bloqueo.

Cuando no está en uso, la información confidencial debe protegerse de la divulgación no autorizada. Cuando se deja en una habitación sin vigilancia, dicha información debe estar asegurada en un contenedor adecuado. La información se puede dejar en un escritorio o en algún otro lugar fácilmente observable sólo si todas las puertas y ventanas a la oficina sin vigilancia están cerradas y bloqueadas durante horas de trabajo.

En caso de una reunión, el director de la reunión se asegurará de que toda la información sea borrada de pizarras, tableros, etc., y cualquier material que quede en la sala al término de la reunión deberá ser recogidos y eliminados de manera segura.

Oficinas privadas:

La información confidencial no se debe dejar de una manera en que las personas no autorizadas puedan ver o tener acceso a ella. En las oficinas privadas, puertas y ventanas deben estar bloqueadas cuando el ocupante del cargo no está en las instalaciones para asegurar el control de acceso. Durante las horas laborales la puerta de la oficina puede estar abierta, sin embargo la información confidencial no debe estar visible a personas no autorizadas, siempre que el ocupante de la oficina deba salir a reuniones la puerta debe quedar cerrada y con seguridad. No está permitido la entrada a una oficina privada por cualquier persona cuando la puerta está cerrada. Las excepciones a esto serían aquellos a los que el permiso le ha sido delegada por el ocupante, basado en el entendimiento de que el delegado está autorizado para todos los niveles de información que pueden estar contenidos dentro de la oficina como parte de las tareas de trabajo normales del delegado por ejemplo, auxiliares administrativos ejecutivos donde el ejecutivo ha concedido específicamente esta excepción.

Almacenamiento de Información Confidencial

Toda información confidencial que no está siendo utilizada por el personal autorizado, ya sea que se encuentre en papel o cualquier otro medio tal como medios de almacenamiento de equipos de cómputo, cd, memorias USB, cintas magnéticas o discos externos deben estar protegidos de manera adecuada, salvaguardándose en archivadores, cajas fuertes u otros medios con mecanismos de bloqueo, o en una oficinas cerrada con seguridad.

Versión	Fecha	Origen
1	31/07/10	Equipo SGSI

4.3.9.3 Otras políticas a implementar. Se recomienda a Sitech de Colombia S.A. diseñar e implementar otras policitas de seguridad de la información que complementen las buenas prácticas, dentro de estas políticas está:

- Política de destrucción de medios magnéticos.
- Política de uso de Dispositivos Móviles.
- Política de Seguridad Física y Áreas Seguras.
- Política de contraseñas.

- Política de protección de información confidencial.
- Política de comunicaciones → Como, cuando, donde, que, quien emite comunicaciones.
- Política de Uso de la red inalámbrica.
- Policita de control de acceso a la red.
- Política de Acceso a los sistemas y gestión de privilegios.
- Política de gestión de medios extraíbles.
- Política de Disposición de medios.
- Política de Manejo de activos de información.
- Política de Antivirus.
- Política de etiquetado y clasificación de la información.
- Política de computación Mobile.
- Política de uso de internet y comunicaciones electrónicas.
- Política de backup de la información.
- Política de Reportes y seguimiento de incidentes de seguridad.

4.3.10 Principales procedimientos a adoptar.

4.3.10.1 Procedimiento de gestión de accesos a los sistemas.

Objetivo.

Este procedimiento regula el proceso de gestión de cuentas de usuarios, incluyendo la determinación y revisión de los permisos de acceso que tienen los usuarios a los sistemas informáticos y a sus estructuras de información.

Alcance.

Alcanza al Jefe de Seguridad de la Información, a los dueños de los activos de Información, al Departamento de TI y al personal autorizado.

Definiciones.

Perfil de Cargo: Ficha descriptiva que incluye las competencias necesarias para el desempeño de cada cargo y responsabilidades que se deberán cumplir.

Incidente: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Cuentas de Usuario: cuenta de usuario para los sistemas.

Estructuras de Información: son las formas en que se accede a la información en los sistemas. Esto es un menú, una carpeta, o un archivo.

Responsabilidades.

El Departamento de TI es responsable de:
Enviar a los Gerentes de Departamento/dueños de activos la lista de permisos de todos los usuarios para el acceso a los activos de información y/o informar de los cambios registrados al menos cada 90 días para mantener la asignación de los permisos de usuarios actualizada.

La Dirección, Gerente de Departamento/dueños de activos, personal autorizado son responsables de: Informar al Departamento de TI los nombres de los empleados que están específicamente autorizados para acceder remotamente a los sistemas de Sitech de Colombia S.A. como así también los accesos que deben tener los usuarios y los cambios que estos deben experimentar según sea necesario.

El Gerente de Departamento/dueño de activo, personal autorizado es responsable de:
Solicitar al Departamento de TI se le adjudiquen al nuevo personal los permisos para los accesos necesarios de acuerdo al perfil de cargo y al egresar personal de la empresa que se le cesen los mismos.

Enviar al Departamento de TI los perfiles de cargo del personal que impliquen cambios en los permisos cuando sea necesario.

El personal es responsable de:
Informar vía e-mail a la persona autorizada de cada departamento con copia al Gerente/dueño de activo y al Departamento de TI cualquier cambio de fechas de licencia/permiso con respecto a las estipuladas en el listado de licencias/permisos del personal.

Configurar su e-mail en caso de licencia la delegación del mismo si correspondiera. En caso de olvido deberá avisar la persona autorizada de su departamento con copia al Gerente/dueño de activo.

Descripción del procedimiento.

Sitech de Colombia provee a todos sus empleados accesos a sus sistemas de información proporcionando una cuenta de usuario único. Las cuentas de usuarios son utilizados a los efectos de restringir los privilegios de acceso de acuerdo con la función, responsabilidades y actividades de cada empleado con acceso al sistema.

Los Gerentes de Departamento/dueños de activos o las personas autorizadas de cada departamento, solicitan al Departamento de TI la creación de los accesos a los diferentes sistemas mediante el uso de correo electrónico, poniendo en el asunto – Gestión de Permisos.

Contratación de personal.
Al contratar personal nuevo, la persona autorizada de cada departamento solicita al Gerente/dueño del Activo y al Departamento de TI que se le adjudiquen los permisos para los accesos necesarios de acuerdo al perfil de cargo.

Licencias.
En el caso de las licencias anuales, la Gerencia de Recursos Humanos envía al Departamento de TI el listado de las licencias de todo el personal. Si en la práctica se registraran cambios a las fechas de licencia estipuladas en el listado de licencias del personal, cada empleado es responsable de comunicar vía e-mail a la persona autorizada de su departamento con copia a su Gerente/dueño de activo y al Departamento de TI. De esta manera, las cuentas son bloqueadas y desbloqueadas por el Departamento de TI por el período de tiempo establecido.

Enfermedad/Ausencia imprevista.
En el caso de enfermedad/ausencia imprevista, cada empleado lo comunica a su Gerente/dueño de activo quien solicitará al Departamento de TI si fuera necesario, que se le otorgue a otro empleado específico el mismo entorno de trabajo con los correspondientes permisos.

Acceso remoto.
La Dirección, el Gerente de Departamento/dueño de activo o la persona autorizada de cada departamento informan al Departamento de TI los nombres de los empleados que están específicamente autorizados para acceder remotamente a los sistemas de Sitech de Colombia.

El Departamento de TI & Proyectos gestiona los correspondientes permisos y futuros controles de los accesos.

El permiso de continuar trabajado a distancia depende del cumplimiento de las políticas y estándares de seguridad aplicables.

El chequeo de correo electrónico por empleados remotos no se considera tele-trabajo, pero debe respetar las mismas regulaciones de seguridad.

Egreso de personal.
Al egresar personal de la empresa, el personal autorizado de cada departamento, o el Gerente/dueño de activo correspondiente solicita al Departamento de TI se le cesen los permisos dando de baja las cuentas correspondientes.

Revisión anual de los permisos de acceso.
El Gerente de TI envía cada 90 días a los Gerentes de Departamento/dueños de activos la lista de permisos del sistema y carpetas compartidas de todos los usuarios para el acceso a los activos de información y/o los cambios registrados en ese período de tiempo; a modo de mantener los derechos de acceso de las cuentas vigentes considerando las posibles variaciones en los perfiles de cargo.

En caso que se suscite cualquier variación durante el año, los Gerentes de Departamentos/dueños de activos informan de los mismos al Departamento de TI.

Medidas disciplinarias.
Cualquier violación/incidente detectado o no cumplimiento de la Política General de Seguridad de la Información, será registrado en el sistema informático correspondiente y puede implicar serias repercusiones para el empleado. Las medidas disciplinarias variarán de acuerdo con la gravedad de la violación, y puede llevar al despido.

Control de versiones

Versión	Fecha	Origen
1	31/07/10	Gerente de IT

4.3.10.2 Procedimiento de control de visitantes al cuarto de comunicaciones.

Objetivo.
Este procedimiento describe cómo se lleva el control de acceso al Cuarto de Comunicaciones.

Alcance.
Alcanza al Jefe de Seguridad de la información y al Departamento de TI.

Definiciones.
Cuarto de Comunicaciones: Lugar físico especial dentro de la empresa en donde se encuentra los computadores principales y servidores. Identificado como zona segura.

Responsabilidades.
El Gerente de TI es responsable de: controlar y registrar el acceso al Cuarto de Comunicaciones.

Descripción del procedimiento.
Todo acceso al Cuarto de Comunicaciones de personas que no pertenezcan al departamento de IT, como personal de empresas de mantenimiento de equipos, soporte, limpieza, etc., deberá quedar registrado en la planilla Control de visitantes al cuarto de comunicaciones. "El cual se puede encontrar en el Anexo H"

Esta planilla se encuentra dentro del Cuarto de Servidores, y se le debe solicitar a la persona que ingresa el registrar la fecha, la hora de ingreso, nombre, documento de identidad, empresa o departamento al que pertenece, motivo de la visita, la hora de su última salida del mismo y su firma. Cuando hayan finalizado su trabajo, se verificará que hayan completado todos los datos solicitados, y el responsable del área de IT firmara en el campo Funcionario que autoriza el ingreso al cuarto de comunicaciones.

Para el control de acceso también se dispone de una cámara de vigilancia ubicada dentro del Cuarto de Comunicaciones, la cual graba todo movimiento dentro del mismo. Se cuenta con un histórico promedio de hasta 30 días.

El control de las grabaciones se hará por solicitud de la Gerencia General o Gerencia de TI.

Documentos de referencia.
Control de visitantes al cuarto de comunicaciones.

Control de versiones.

Versión	Fecha	Origen
1	31/07/10	Gerente de IT

4.3.10.3 Otros procedimientos a adoptar. Se recomienda a Sitech de Colombia adoptar lo procedimientos sin limitarse a la siguiente lista:

- Mantenimiento preventivo y correctivo de recursos informáticos.
- Control de acceso a la instalaciones.
- Gestión de soporte a usuarios.
- Gestión de copias de seguridad.
- Eliminación de medios de almacenamiento e información.
- Gestión de cambios en los sistemas e instalaciones de procesamiento de información.
- Asignación de equipos móviles.
- Revisión de registros de acceso y uso de los sistemas.
- Realización de respaldos y recuperación de la información.
- Verificación de respaldo de información.
- Manejo de activos de información.
- Plan de continuidad de negocio.
- Diagrama de red.

5. CONCLUSIONES

De acuerdo con la hipótesis formulada se puede concluir que:

- Al implementar un SGSI Sitech de Colombia SA puede identificar las vulnerabilidades de sus activos de información planteando controles para minimizar la exposición a niveles aceptables por la compañía.

- Resultado del análisis de brecha ISO 27001:2013 se registraron 48 cumplimientos de los 155 aspectos evaluados, lo cual hace referencia al estado actual de Sitech con respecto a un SGSI implementado y nos indica que tiene bases para iniciar con la fase de planeación.

- Según el análisis de riesgos y el plan de tratamiento de los mismos, se identificó que los activos más importantes para la compañía son el personal y la información en sus diferentes medios de presentación, ya sea en físico, digital o medios de almacenamiento y respaldo, por lo cual es muy importante ejecutar los controles señalados para minimiza los riesgos de seguridad que pueden afectar estos activos.

- Las principales vulnerabilidades encontradas corresponden a la ausencia de procedimientos, controles y políticas formales que le permitan a los empleados tener un marco de referencia para la seguridad de la información, estas vulnerabilidades tienen un peso del 23 % con respecto a la totalidad.

- El 5 % de los riesgos encontrados están en un rango aceptable, el 69 % en un rango moderado y el 30 % en un rango inaceptable. Aunque la organización acepta los riesgos en estado aceptable y moderado, es importante que Sitech implemente controles para minimizar los riesgos moderados los cuales tienen el mayor porcentaje con respecto al total identificado.

- Aunque la declaración de aplicabilidad nos revela que Sitech tiene implementados 27 controles de la norma ISO 27001:2013, como resultado de este planteamiento se definió que se requiere implementar 44 controles adicionales para tratar 52 vulnerabilidades en 118 activos que pueden ser atacados por 31 amenazas.

- Los controles que ayudan a mitigar la mayoría de los riesgos de seguridad son el A.12.1.1 y A.12.1.2 de la norma ISO 27001:2013, los cuales corresponden al 30 % de los riesgos identificados.

- La realización de este proyecto fue un paso inicial en la conciencia de cada integrante de Sitech, pues acerco un poco a la realidad el estado de la compañía con respecto a la seguridad de la información y evidencio los impactos posibles de no implementar controles para minimizar los riesgos.

6. RECOMENDACIONES

- Es evidente que Sitech debe implementar un plan de concienciación en sus empleados, ya que este es el eslabón más débil en la probabilidad de ocurrencia de los riesgos identificados. Personal capacitado y entrenado en temas relacionados en la seguridad de la información minimizan la brecha de seguridad en la empresa.

- Se recomienda a Sitech implementar las políticas, procedimientos y controles señalados en el plan de tratamiento de riesgos para disminuir la probabilidad de ocurrencia de los mismos y por ende el posible impacto para la organización.

- El sistema de gestión de seguridad de la información debe ser impulsado por la alta gerencia de Sitech, esto puede asegurar que se cumplan con mayor eficacia los controles, procedimientos y políticas implementadas.

- La conciencia de la seguridad de la información debe ser abordada desde el proceso de contratación, especificando los deberes y responsabilidades de cada empleado que es contratado en Sitech, esto debería estar por escrito y ser aceptado por cada persona al firmar el contrato de trabajo.

- Es esencial para Sitech implementar un mecanismo de registro, seguimiento y control de los incidentes de seguridad de la información.

- Adoptar la política de seguridad de la información que se establece en este planteamiento, difundiéndola y socializándola a todo el personal y partes interesadas.

- Instaurar la estructura propuesta para el manejo adecuado del tratamiento de la seguridad de la información, asignando roles y responsabilidades.

BIBLIOGRAFÍA

Dejan Kosutic, Ciber seguridad en 9 pasos, el manual sobre seguridad de la información para el gerente, Primera edición del 2012, Publicado por EPPS Services Ltd, Zabreg disponible en http://www.iso27001standard.com/

Humberto Serna Gómez, Gerencia Estratégica, Teoría – metodología – Alineamiento, implementación y mapas estratégicos, índices de gestión, 10 Edición. 2015.

Norma técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnologías de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos, Primera actualización, Editada 2013-12-20.

Norma técnica Colombiana NTC-ISO-IEC 27005:2009, Tecnologías de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información, Editada 2009-09-01.

BIBLIOGRAFÍA COMPLEMENTARIA

http://advisera.com/27001academy/

http://advisera.com/27001academy/es/blog/2010/07/21/cuatro-beneficios-clave-de-la-implementacion-de-la-norma-iso-27001/

http://blog.firma-e.com/beneficios-de-implantar-un-sgsi-en-su-empresa/

http://blog.nerion.es/los-beneficios-de-la-implantacion-de-un-sgsi/

http://www.iso27000.es/

http://www.normas-iso.com/categoria/preguntas/iso-27001/beneficios-iso-27001

http://www.pmg-ssi.com/2015/09/beneficios-iso-iec-27001-2013/

http://www.sbqconsultores.es/iso-27001-que-beneficios-nos-aporta-implantarla/

http://www.tyd.es/ISO27000-6.html

ANEXOS

Anexo A. Análisis externo Sitech

DIAGNOSTICO EXTERNO SITECH

¿Cuáles son los aspectos económicos, sociales, culturales, geográficos, demográficos, políticos y legales que afectan la organización?
Producto interno bruto, tasas de interés de captación y colocación, disponibilidad de crédito, inflación, devaluación, patrones y cambios en el consumo, balanza cambiaria, ingreso per cápita, impuestos, salario mínimo, tamaño del mercado, pronósticos económicos, déficit presupuestarios, políticas monetarias, fiscales y cambiarias, confianza en el gobierno, relaciones internacionales, ley tributaria, ley laboral, reforma financiera, aranceles, leyes de protección al medio ambiente,
Económicos: disponibilidad de crédito, patrones y cambios en el consumo, impuestos, tamaño del mercado, políticas monetarias, fiscales y cambiarias. Sociales, culturales, geográficos y demográficos: estilos de vida. Legales: Reforma financiera, actividades terroristas.
Más empleados certificados y aptos para salir al mercado, innovación
Inflación, disponibilidad de crédito, competencia.
Inflación, disponibilidad de créditos
Producto interno bruto, ley laboral
Privatización al consumidor , niveles educativos, impuestos
¿Cuáles son las variables económicas, sociales, culturales, geográficas, demográficas, políticas y legales que debe evaluar la empresa?
Producto interno bruto, tasas de interés de captación y colocación, disponibilidad de crédito, inflación, devaluación, patrones y cambios en el consumo, balanza cambiaria, ingreso per cápita, impuestos, salario mínimo, tamaño del mercado, pronósticos económicos, déficit presupuestarios, políticas monetarias, fiscales y cambiarias, confianza en el gobierno, relaciones internacionales, ley tributaria, ley laboral, reforma financiera, aranceles, leyes de protección al medio ambiente,
Económicos: patrones y cambios en el consumo. Sociales, culturales, geográficos y demográficos: estilos de vida. Legales: Leyes de protección al medio ambiente.
Tamaño del mercado
Patrones y cambios en el consumo, tamaño del mercado, ley tributaria, impuestos
Patrones y cambios en el consumo, tamaño del mercado, , ley tributaria, impuestos
Número de escuelas, colegios y universidades
Impuestos, devaluación, políticas de inversión
¿Cuáles son las fuentes de información para el análisis de las variables clave externas?
Todos y cada uno de los medios de comunicación masiva
Legislación y reformas, e inflación.
Competencia con más opciones en prestación de servicios
Reformas financieras, políticas monetarias,
Reformas financieras, políticas cambiarias y monetarias.
Estadísticas, reportes oficiales del estado
Legalización reformas, e inflación

¿Cuáles son las tendencias que presentan las variables económicas, sociales, culturales, geográficas, demográficas, políticas y legales que evalúa la empresa?
No hay una tendencia definida, se debe realizar un análisis exhaustivo de cada una de ellas para determinar la tendencia.
Tamaño del mercado, niveles educativos y ley tributaria.
Prestación de servicios e innovación. Servicios en economizar de los servicios
Índice de desempleo, salario mínimo, tamaño del mercado.
Índice del desempleo, salario mínimo, tamaño del mercado
La tendencia es al aumento
'Tamaño del mercado, niveles educativos
¿Cuáles son las amenazas económicas, sociales, culturales, geográficas, demográficas, políticas y legales, a las que está expuesta la organización, con base en las variables evaluadas?
Las amenazas son todas y cada una de las que puedan llegar a generar cambios significativos en cada una de las variables citadas anteriormente.
Pronósticos económicos, disponibilidad del crédito, devaluación, inflación, desempleo.
Inflación y actividad terrorista.
Quien no innova tiende a desaparecer
Leyes de protección al medio ambiente e inflación, actividad terrorista
Pronósticos económicos, disponibilidad del crédito, inflación
¿Cuáles son las oportunidades económicas, sociales, culturales, geográficas, demográficas, políticas y legales, que favorecen la organización, con base en las variables evaluadas?
Todas aquellas que permitan encausar de manera adecuada el crecimiento de la compañía.
Crecimiento del mercado, número de escuelas y universidades, salud y seguridad.
Nicho de mercados especializados
Estilos de vida, población total, leyes laborales y reformas tributarias.
Estilos de vida, población total, leyes laborales, y reformas tributarias.
Aumento de oportunidades con el incremento de mercado en el sector educativo
Tamaño del mercado, número de escuelas colegios y universidades, salud y seguridad
¿La empresa se considera amenazada por su entorno?
Actualmente, la empresa se considera vulnerable al entorno socioeconómico en el cual desempeña sus actividades diarias en todos y cada uno de sus aspectos.
En infraestructura quizás por los temas de terrorismo en nuestro país, en nuestra misión también pues tenemos mucha competencia y los cambio en los gustos de las empresas y su gente.
N/a
Si
Si
El cambio del dólar es una amenaza
A nivel de infraestructura si debido a las actividades terroristas y a nivel tecnológico si debido a que el mundo tecnológico se encuentra en constante cambio

¿El entorno de la empresa es favorable para su desarrollo futuro?
Totalmente, así como estamos vulnerables a las amenazas del entorno, nos encontramos en igualdad de condiciones para detectar oportunidades y hacerlas fortalezas para nuestro core de negocio.
Claro, está en constante crecimiento.
Por supuesto.
Si
Si
Es favorable
Demasiado ya que el sector tecnológico es un sector de demasiada demanda y de constante crecimiento lo que permitirá el desarrollo de nueva tecnología para los consumidores
¿Cuáles son las clases de tecnología que se utilizan en la entidad?
Tecnología blanda, tecnología de equipo, tecnología de operación, tecnología de producto y tecnología limpia
Tecnología flexible, fija, dura, blanda, de equipo, de operación, y limpia.
Software, hardware, partes y algunos servicios
Inalámbrica, acceso remoto, wifi, internet, Ethernet.
Inalámbrica, acceso remoto, wifi, internet, Ethernet
Tele mercadeo
Tecnología fija, tecnología flexible, tecnología blanda
¿Que se piensa en la organización con respecto a la tecnología?
En términos generales en la organización se piensa que la tecnología solo hace referencia a los productos y servicios que ofertamos.
Es el conocimiento técnico que tiene cada una de las personas para el desarrollo de sus funciones en pro de la compañía.
Debe buscar más integralidad
Que es el futuro de la humanidad
Que es el futuro de la humanidad en comunicación, avances y conocimientos
Se debe utilizar para estar actualizados
La tecnología es un mundo de diversidad y herramientas que facilitan el trabajo y permiten el desarrollo de una compañía a menor costo
¿Es importante la tecnología en el giro del negocio de la empresa?
Por supuesto que es importante dado que a medida que evoluciona, debemos conocer las herramientas que fortalezcan nuestro proceso de venta.
Claro.
Por supuesto
Súper importante es nuestro núcleo.
Claro
Es muy importante
Es de vital importancia ya que favorece la reducción de los costos y adicional es un mercado que siempre se encontrara en constante demanda

¿Cuál es el nivel tecnológico que usa la organización?
En mi concepto el nivel tecnológico que se maneja en la organización es medio, dado que siendo proveedores de tecnología deberíamos estar más a la par de la misma.
Alto.
Media
Alto.
Alto
Alto
Nos encontramos en un nivel medio ante grandes organizaciones dando por concreto un nivel de tecnología smbi
¿Es esencial la tecnológica como elemento diferenciador de la compañía?
Claro que si, en nuestro medio de desempeño es fundamental contar con la tecnología como elemento diferenciador, dado que el grado de innovación que podamos aplicar a cualquier solución puede ser determinante en la toma de decisiones cliente al momento de asignar la compra.
Si.
Claro con innovación
Súper esencial
Claro
Es muy importante para lograr buen desempeño
Obviamente ya que no solo nos encargamos de vender tecnología sino que también la utilizamos como medio o herramienta para satisfacer las necesidades de la compañía
¿Es un objetivo para la organización poseer tecnología de punta?
Debería serlo dado que es el core de nuestro negocio, pero es una decisión netamente gerencial.
Si.
N/a
Si
Siempre.
Si
Total ya que al momento de poseer dicha tecnología la compañía seria líder del mercado y se posesionaria como una de las mejores o en su defecto la mejor
¿Cuál es el nivel tecnológico de los insumos comprados por la organización?
El nivel tecnológico en mi concepto es medio, dado que conocemos el mercado y sabemos lo que actualmente se está usando en el mismo; aún tenemos obsolescencia en la infraestructura con la que contamos actualmente.
Tecnología flexible.
Bueno
De punta
Alto
Alto
A nivel de calidad excelente y a nivel de innovación se encuentra en promedio ya que no somos la única compañía que se encarga de comprar y comercializar el mismo producto

¿Es crítico el nivel tecnológico de los insumos adquiridos?
No es crítico, pero reitero podríamos contar con insumos más acordes a la tecnología actual.
Claro.
No
No
No
No
No para nada ya que critico sería un producto defectuoso o que no cuente con las normas establecidas por la organización
¿Cómo afecta la tecnología los procesos core de la organización?
En este momento nos afecta en las entregas de propuestas por caídas de internet, cambios en las credenciales de acceso al servidor sin dar aviso al usuario, implementación de aplicativos que hacen ralentizar los equipos, alta dependencia del área de IT para dar solución a los requerimientos que se presentan.
Cada una de las personas de la organización debe tener conocimientos y experiencia para que pueda dar ejecución a los procesos y razón de ser de la compañía.
Menos tiempo
Tiempo de entrega, servicio al cliente y eficiencia.
Tiempo de entrega, satisfacción de nuestros clientes, oportuno servicio a cada uno de nuestros clientes
Ayudan al mejor desempeño
A nivel de presupuesto, y desarbolo e innovación que nos impiden competir con otras organizaciones
¿De qué manera se afecta la satisfacción del cliente frente al nivel tecnológico de los productos vendidos por la empresa?
La satisfacción del cliente se ve afectada en ocasiones en las cuales no se brinde una correcta asesoría y los productos ofertados no satisfagan en su totalidad la necesidad del cliente.
Se puede afectar al momento de una mala asesoría, invertir en productor que no cumplan con la necesidad.
En 100% confianza
Alto porque siempre quedan satisfechos
Alto
Es proporcional
Cuando el producto que se vende es defectuoso y no satisface las necesidades del cliente
¿Es la tecnología una variable dependiente o independiente del nivel de ventas y utilidades de la organización?
Es una variable dependiente, es factor fundamental para lograr la venta que por ende genera utilidad para la compañía.
Dependiente.
Dependiente
Si
Si
Dependiente
Dependiente ya que siempre será este medio el que permitirá la entrada de dinero para la organización

¿Qué tecnologías deben utilizarse para alcanzar los objetivos empresariales?
Excepcionalmente la tecnología de punta contribuye de manera directa a la consecución de los objetivos trazados por la organización.
Tecnología flexible, blanda, de equipo, de operación.
N/a
Tecnología de última generación
De punta.
Redes sociales para contactar clientes
Tecnología que brinde coberturas a nivel nacional e internacional y en donde todo individuo pertenezca a ese vínculo como tecnología satelital
¿Cuál es el grado de obsolescencia de la tecnología usada por la organización?
Dado que la vida útil de la tecnología en general es de un promedio de 3 años, podríamos decir que el grado de obsolescencia en la organización en términos porcentuales es de un 70%
Baja.
N/a
Cero
0
El nivel de obsolescencia es bajo
Nivel bajo
¿Cuál ha sido la evolución tecnológica de la compañía y sus proveedores?
Como conocedor del proceso de crecimiento de la compañía puedo decir que la evolución tecnológica tanto de la organización como de los proveedores ha sido muy favorable en el tiempo de operación hasta la fecha.
Evolución en tecnología blanda alta.
N/A
Siempre vamos de la mano de todas las actualizaciones de la tecnología.
Satisfactoria y vamos de mano para las necesidades del cliente
Ha avanzado a medida que la tecnología llega al país
Evolución de comunicación y de repuesta a las partes interesadas
¿Cuánto ha invertido la empresa en tecnología?
Desconozco las cifras
$38'000.000
N/a
$38.000.000
$ 38.000.000.oo
Lo necesario para que cada colaborador interactúe y saque ventaja de la tecnología
El 80 por ciento del capital con el que cuenta
¿Cuánto espera invertir en el futuro?
Desconozco la información
$20'000.000
N/a
$80.000.000
$ 80.000.000.oo
La inversión será grande para la proyección
El 80 por ciento del capital que en su momento tenga la organización

¿Cuánto debería invertir?
Lo necesario para garantizar la operación de la compañía, enfocados en la consecución de los objetivos gerenciales.
$28.000.000
0,8
$40.000.000
$ 35.000.000.oo
Debería invertir un poco más en i&d
La mitad de los recursos con lo que cuenta
¿Cuáles son las prioridades de inversión en tecnología?
Nuevas instalaciones
Infraestructura, compras en línea al igual servicio al cliente inmediato.
N/a
Equipos actualizados
Equipos
La prioridad es para consumo interno, mas no para investigación
Suministros para solventar los Outsourcing prestados y quipos
¿Qué inversiones tecnológicas deberían reducirse o eliminarse?
Ninguna
Reducir las cámaras de seguridad internas.
N/a
Ninguna porque todo es necesario
Ninguna
Las inversiones hechas hasta el momento han sido justas y necesarias
Inversiones en objetos obsoletos como teclados mouse que ya no son el foco de venta de la empresa
¿Cuál es la tasa interna de retorno de la inversión tecnológica?
Debe proyectarse de acuerdo con la inversión que se pretende hacer vs. La rentabilidad que se espera obtener a través de esa inversión.
0,9
N/a
1
1
30 %
El 90 porciento
¿Cuál es la tasa interna de retorno de la inversión tecnológica?
Conozco algunos competidores en los cuales el nivel tecnológico es mucho mayor al nuestro.
Alto.
N/a
Bueno
Bueno.
El nivel es alto
Al mismo promedio al que nos encontramos nosotros un nivel smbi

¿Cuánto ha invertido la competencia en tecnología?
Desconozco las cifras.
Bastante.
N/a
Un valor menos que nosotros
$ 31.000.000.oo
La inversión es racional a las condiciones de la moneda de transacciones extranjeras
El 70 por ciento de los recursos con lo que cuentan
¿Cuál es el nivel tecnológico de la empresa, dentro del ámbito competitivo en el cual se desempeña?
Me atrevería a decir que estamos ubicados en un nivel medio.
Tecnología flexible y de operación.
N/a
Excelente
Bueno.
El nivel es medio
Es un nivel igual a la que manejamos nosotros la diferencia son los costos de venta que ofrece al cliente final
¿Cuáles son las opciones tecnológicas de la compañía?
Desconozco la información sobre el enfoque que quiera dar la gerencia a la implementación de tecnología en un futuro.
Tecnología fija y dura.
N/a
Redes sociales
CRM, redes sociales, help desk,
Las opciones son de crecimiento en investigación
Tecnología fija y creación de software
¿Cuáles tecnologías ha implementado? ¿Por qué?
Recientemente no se han realizado cambios significativos.
Tecnología flexible, porque tenemos tanto elementos físicos y conocimientos para realizar nuestra actividad comercial.
N/a
Help desk, soporte remoto, porque con eso se lleva las métricas de los procesos realizados
Help desk , soporte remoto, porque se llevan las métricas de cada una de las necesidades de nuestros clientes a diario
Virtualización, ERP, wifi, móvil, porque se han requerido para facilitar el desempeño de los empleados
Tecnología de valor agregado porque se engancha una oportunidad de negocio

¿Cuáles no ha implementado? ¿Por qué?
Desconozco los cambios que quiera implementar la gerencia.
Tecnología dura, porque no se han creado productos materiales.
N/a
CRM porque hasta la fecha no la habíamos necesitado
CRM, porque la necesidad hasta la fecha no la había requerido, en compras y ventas.
Backup en la nube, por costos y funcionalidad
Tecnología de creación flexible porque no hay el suficiente personal capacitado para desarrollar dicha tecnología y lo más importante renovarla y mantenerla
¿Cuáles son las barreras representativas para mejorar el nivel tecnológico de la empresa?
Considero que principalmente es el presupuesto para renovación tecnológica.
Negación al cambio por parte de las personas que integran la compañía. No contar con el personal idóneo para cada cargo. Cambios repentinos e inesperados de la industria.
N/a
No hay
Ninguna.
Prioridades de inversión
El factor económico y el factor sector ya que la mejor tecnología no se fabrica dentro de nuestro sector si no lejos de el

Anexo B. Análisis interno Sitech

DIAGNOSTICO INTERNO SITECH

CAPACIDAD DIRECTIVA

		FORTALEZA			DEBILIDAD			IMPACTO		
#	***Question***	**ALTO**	**MEDIO**	**BAJO**	**ALTO**	**MEDIO**	**BAJO**	**ALTO**	**MEDIO**	**BAJO**
1	IMAGEN CORPORATIVA, RESPONSABILIDAD SOCIAL	2	3	1	1			3	3	1
2	USO DE PLANES ESTRATÉGICOS, ANÁLISIS ESTRATÉGICO	1	2		1	1	2	4	2	1
3	EVALUACIÓN Y PRONOSTICO DEL MEDIO	1	3	1	1		1	3	4	
4	VELOCIDAD DE RESPUESTA A CONDICIONES CAMBIANTES	1	2	4				3	4	
5	FLEXIBILIDAD DE LA ESTRUCTURA ORGANIZACIONAL	1	3	1			1	4	2	1
6	COMUNICACIÓN Y CONTROL GERENCIAL	2	3	1	1			3	4	
7	ORIENTACIÓN EMPRESARIAL	1	4	1		1		3	4	
8	HABILIDAD PARA ATRAER Y RETENER GENTE ALTAMENTE CREATIVA	1	2	3	1			3	4	
9	HABILIDAD PARA RESPONDER A LA TECNOLÓGICA CAMBIANTE	1	5	1				1	6	
10	HABILIDAD PARA MANEJAR LA INFLACIÓN		3	4					6	1
11	AGRESIVIDAD PARA ENFRENTAR LA COMPETENCIA	4	1	1	1			4	3	
12	SISTEMAS DE CONTROL	1	2	1	2		1	3	3	1
13	SISTEMAS DE TOMA DE DECISIONES	2	1	2	1		1	3	4	
14	SISTEMAS DE COORDINACIÓN		3	2	2			2	5	
15	EVALUACIÓN DE GESTIÓN		4	1	1		1	2	5	

CAPACIDAD TECNOLÓGICA

		FORTALEZA			DEBILIDAD			IMPACTO		
#	Question	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO
1	HABILIDAD TÉCNICA	2	4		1			1	6	
2	CAPACIDAD DE INNOVACIÓN	2	3	1		1		4	3	
3	NIVEL DE TECNOLOGÍA UTILIZADO EN LOS SERVICIOS Y PRODUCTOS	3	3	1				3	4	
4	FUERZA DE PATENTES Y PROCESOS		3	1	1	1	1	2	2	3
5	EFECTIVIDAD DE LA PRODUCCIÓN Y PROGRAMAS DE ENTREGA		5	1	1			1	6	
6	VALOR AGREGADO AL PRODUCTO	3	3	1				5	2	
7	INTENSIDAD DE MANO DE OBRA EN LOS SERVICIOS Y PRODUCTOS	2	3	2				2	5	
8	ECONOMÍA DE ESCALA	1	3	1		2		2	3	2
9	NIVEL TECNOLÓGICO	4	1	2				3	4	
10	APLICACIÓN DE TECNOLOGÍA DE COMPUTADORAS	5	1	1				3	3	1
11	NIVEL DE COORDINACIÓN E INTEGRACIÓN CON OTRAS ÁREAS		5	1	1			4	2	1
12	FLEXIBILIDAD DE LOS SERVICIOS Y LA PRODUCCIÓN		5	2				1	6	

CAPACIDAD DEL TALENTO HUMANO

		FORTALEZA			DEBILIDAD			IMPACTO		
#	Question	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO
1	NIVEL ACADÉMICO DEL TALENTO		5	1		1		3	4	
2	EXPERIENCIA TÉCNICA		5	1	1			4	3	
3	ESTABILIDAD	2	4				1	3	3	1
4	ROTACIÓN		4		1	1	1	3	4	
5	ABSENTISMO	1	4	1	1			2	5	
6	PERTENENCIA	1	4	1	1			5	2	
7	MOTIVACIÓN	1	3	2	1			3	4	
8	NIVEL DE REMUNERACIÓN		5	2				2	5	
9	ACCIDENTALIDAD	1	1	5				3	1	3
10	RETIROS		3	2	1	1		2	5	
11	ÍNDICES DE DESEMPEÑO		5	1	1			4	3	

CAPACIDAD COMPETITIVA

		FORTALEZA			DEBILIDAD			IMPACTO		
#	Question	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO
1	FUERZA DE SERVICIOS, PRODUCTO, CALIDAD, EXCLUSIVIDAD	1	5	1				3	4	
2	LEALTAD Y SATISFACCIÓN DEL CLIENTE	4	3					5	1	1
3	PARTICIPACIÓN EN EL MERCADO	3	1	3				4	1	2
4	BAJOS COSTOS DE DISTRIBUCIÓN Y VENTAS	2	2	2		1		3	2	2
5	USO DE LA CURVA DE EXPERIENCIA	1	3	2			1	1	5	1
6	USO DEL CICLO DE VIDA DEL PRODUCTO Y DEL CICLO DE REPOSICIÓN	1	3	2		1		1	5	1
7	INVERSIÓN EN I&D PARA DESARROLLO DE NUEVOS SERVICIOS Y PRODUCTOS	1	3	1	1	1		2	3	2
8	GRANDES BARRERAS EN ENTRADA DE SERVICIOS Y PRODUCTOS EN LA COMPAÑÍA	2	2	2		1		1	3	3
9	VENTAJA SACADA DEL POTENCIAL DE CRECIMIENTO DEL MERCADO	3	2	1	1			3	3	1
10	FORTALEZA DEL (LOS) PROVEEDOR (ES) Y DISPONIBILIDAD DE INSUMOS	4	2	1				3	3	1
11	CONCENTRACIÓN DE CONSUMIDORES	1	4	2				4	2	1
12	ADMINISTRACIÓN DE CLIENTES	2	2	3				3	3	1
13	ACCESO A ORGANISMOS PRIVADOS Y PÚBLICOS	2	2	3				4	2	1
14	PORTAFOLIO DE PRODUCTOS	3	4					4	2	1
15	PROGRAMAS DE POSVENTA	2	2	2			1	2	4	1

CAPACIDAD FINANCIERA

		FORTALEZA			DEBILIDAD			IMPACTO		
#	Question	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO
1	ACCESO A CAPITAL CUANDO LO REQUIERE	2	3	1	1			6	1	
2	GRADO DE UTILIZACIÓN DE SU CAPACIDAD DE ENDEUDAMIENTO	3	3		1			6	1	
3	RENTABILIDAD , RETORNO DE LA INVERSIÓN	2	2	2	1			4	3	
4	LIQUIDEZ, DISPONIBILIDAD DE FONDOS INTERNOS	1	5		1			4	3	
5	COMUNICACIÓN Y CONTROL GERENCIAL	1	3	2	1			4	3	
6	HABILIDAD PARA COMPETIR CON PRECIOS	2	3	2				6	1	
7	INVERSIÓN DE CAPITAL, CAPACIDAD PARA SATISFACER LA DEMANDA		6	1				3	4	
8	ESTABILIDAD DE COSTOS		5	2			1	1	4	1
9	HABILIDAD PARA MANTENER EL ESFUERZO ANTE LA DEMANDA CÍCLICA	1	5	1				2	4	1
10	ELASTICIDAD DE LA DEMANDA CON RESPECTO A LOS PRECIOS	1	4	2				2	5	

Anexo C. Inventario de activos de información

PROCESO	DUEÑO / RESPONSABLE	CATEGORÍA	TIPO	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
GESTIÓN FINANCIERA	CARLOS NEUTO	HARDWARE	SOPORTE	CAJA FUERTE	4	4	4	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	IMPRESORAS	3	3	2	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	ACCESS POINT	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	UPS	4	4	3	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE APLICACIONES	4	4	3	4
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	TELÉFONO CELULAR	3	3	2	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SISTEMA DE BAKCUP	4	4	4	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	DISCO DURO PARA BACKUP	4	4	4	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	DVR	4	4	4	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	TELÉFONOS CELULARES	3	3	2	2
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	CAMIONETA	3	3	2	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	MOTO	3	3	2	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE ARCHIVOS	4	4	3	4
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	COMPUTADORES DEL ÁREA FINANCIERA	3	4	4	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	PLANTA TELEFÓNICA	4	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	COMPUTADORES DEL ÁREA LOGÍSTICA	3	4	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	TOKEN BANCO	4	5	5	5
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	SISTEMA DE VIGILANCIA	4	4	2	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SWITCHES	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	ROUTER	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	PARQUE INFORMÁTICO	4	4	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO	LUGAR	SOPORTE	OFICINAS ADMINISTRATIVAS	4	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	BODEGA DE ALMACENAMIENTO	4	4	4	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	CUARTO DE COMUNICACIONES	4	4	4	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	CUARTO DE SERVICIO TÉCNICO	4	4	2	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO	ORGANIZACIÓN	PRIMARIO	INFORMES DEL ÁREA LOGÍSTICA	3	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	CONTRATOS DE SERVICIOS	4	4	4	5
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	FACTURA DE PROVEEDOR	3	4	2	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	DOCUMENTOS DE GARANTÍAS	4	4	3	4
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	PEDIDOS DE COMPRA	3	4	4	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	PEDIDOS DE VENTA	3	4	4	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	PROCEDIMIENTO DE GARANTÍAS	3	4	2	3
GESTIÓN FINANCIERA	MARISOL VELA		PRIMARIO	PAGO A PROVEEDORES	4	4	4	5
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	ESTADOS FINANCIEROS	4	5	4	3

PROCESO	DUEÑO / RESPONSABLE	CATEGORÍA	TIPO	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	VERIFICACIÓN DE DATOS	4	4	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CONSIGNACIONES	3	4	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CONCILIACIONES BANCARIAS	3	5	4	4
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	COMPROBANTES DE NOMINA	3	5	5	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	INVENTARIO DE ACTIVOS FIJOS	3	5	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	INFORMES DE REVISORÍA FISCAL	4	5	5	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	CONTINUIDAD DE NEGOCIO	4	5	5	5
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	EXTRACTOS BANCARIOS	3	5	4	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	ORDENES DE COMPRA	3	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	REMISIONES	2	3	3	4
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	IMPUESTOS	4	5	4	4
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	INFORMES FINANCIEROS	4	5	4	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	CREACIÓN DE CREDENCIALES (AD, CORREO, ERP)	3	3	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	LEGALIZACIÓN DE GASTOS	3	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	MANUALES DE USUARIO	4	3	2	3
GESTIÓN FINANCIERA	MARISOL VELA		PRIMARIO	CREACIÓN DE CUENTAS CONTABLES	3	5	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	ANTICIPOS	2	4	2	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	INVENTARIO DE ACTIVOS ETNOLÓGICOS	2	4	4	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	PLANOS DEL EDIFICIO	3	3	2	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	INDICADORES DE MEDICIÓN DE IT	3	3	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CUSTODIA DE BIENES	4	5	4	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	FACTURA DE CLIENTE	3	4	2	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	PARAFISCALES	3	4	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	INDICADORES DE MEDICIÓN	3	5	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	REGISTRO DE PROVEEDORES	3	4	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	REGISTRO DE CLIENTES	3	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	REGISTROS DE CORRESPONDENCIA	3	3	3	2
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	REPORTE DE VENTAS	3	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	ACTAS DEL COMITÉ DE COMPRAS	2	3	3	2
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	COMPROBANTES DE DEVOLUCIÓN DE MERCANCÍA	2	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	COMPROBANTES DE ENTRADA POR DEVOLUCIÓN	2	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	COMPROBANTES DE RECIBO DE MERCANCÍA	2	4	3	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	DIAGRAMA DE RED	3	4	4	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	DIAGRAMA DE DATACENTER	3	4	4	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	DOCUMENTACIÓN DE SISTEMAS DE INFORMACIÓN	3	3	3	3

PROCESO	DUEÑO / RESPONSABLE	CATEGORÍA	TIPO	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	INVENTARIO DE SISTEMAS DE INFORMACIÓN	3	3	3	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	INVENTARIO DE SISTEMAS DE INFORMACIÓN CRÍTICOS	3	3	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	INFORMACIÓN FINANCIERA DE CLIENTES	3	4	5	4
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	DOCUMENTOS PARA EL ESTUDIO DE CRÉDITO	3	4	5	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	PLANILLA DE RECORRIDO DIARIO - RUTA	3	3	3	4
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	INVENTARIO DE VEHÍCULOS	2	3	2	2
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	COMPROBANTES DE CAUSACIÓN	4	5	4	4
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	DIRECTORIO TELEFÓNICO DE CLIENTES Y PROVEEDORES	4	4	2	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CUENTAS POR PAGAR	3	4	4	4
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CUENTAS POR COBRAR	3	4	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CONTRATOS	3	5	4	4
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	BACKUP DE ARCHIVOS FINANCIERA	4	5	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	REGISTRO DE APORTES SOCIALES	3	4	3	3
RECURSOS HUMANOS	MARISOL VELA	PERSONA	PRIMARIO	EMPLEADOS	4	4	4	5
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	PERSONAL DE MENSAJERÍA	4	4	3	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	INGENIEROS DE SOPORTE	4	4	3	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	INGENIEROS DE SOPORTE	4	4	3	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	PERSONAL DE OUTSOURCING TÉCNICO	4	4	3	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	PERSONAL DE OUTSOURCING TÉCNICO	4	4	3	5
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	PERSONAL DE OUTSOURCING TÉCNICO	4	4	3	5
GESTIÓN FINANCIERA	MARISOL VELA	RED	SOPORTE	INTERNET - PORTAL DE BANCOS	4	4	5	3
GESTIÓN FINANCIERA	CARLOS NEUTO		PRIMARIO	CARPETA COMPARTIDA FINANCIERA	3	5	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	SERVICIO DE TELEFONÍA	4	3	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	SERVICIO DE INTERNET	4	4	4	3
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	RED DE DATOS	5	4	4	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	SERVICIO DE TELEFONÍA	3	4	2	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	RED DE DATOS	5	4	2	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	CCTV	5	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SERVICIO DE CORREO ELECTRÓNICO	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	RED WIFI	3	3	2	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	INTERNET	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	RED DE ENERGÍA REGULADA	4	4	2	4
GESTIÓN FINANCIERA	CARLOS NEUTO	SOFTWARE	SOPORTE	MODULO FINANCIERO ERP WORLD OFFICE	4	4	4	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	MODULO DE LOGÍSTICA ERP WORLDOFFICE	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	BASE DE DATOS DIRECTORIO ACTIVO	3	4	4	3

PROCESO	DUEÑO / RESPONSABLE	CATEGORÍA	TIPO	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	ERP WORLDOFFICE	3	4	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	SUITE OFFICE	4	4	3	3
GESTIÓN FINANCIERA	CARLOS NEUTO		SOPORTE	CORREO ELECTRÓNICO	3	5	5	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SOFTWARE DE TICKETS	2	3	3	2
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	PAGINA WEB	4	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	BASE DE DATOS DE CLIENTES	3	4	4	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	CONSOLA DE ANTIVIRUS	3	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SOFTWARE UNIFI	4	4	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	SERVIDOR VIRTUAL DE TICKETS	4	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		SOPORTE	SUITE OFFICE - EXCEL	2	3	2	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	CÓDIGO FUENTE DE SISTEMAS O DESARROLLOS	3	3	3	3
GESTIÓN DE IT	HERIBERTO CEBALLOS		SOPORTE	HYPER-V	3	4	3	3
GESTIÓN LOGÍSTICA	RAFAEL PALACINO		PRIMARIO	BASE DE DATOS DE PROVEEDORES	3	4	3	4
GESTIÓN DE IT	HERIBERTO CEBALLOS		PRIMARIO	BASE DE DATOS ERP	4	4	4	4

ANEXO D

Reporte de Alertas de Seguridad de la Aplicación GLPI

Sitech de Colombia SAS

X-Frame-Options Header Not Set

Descripción

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Riesgo

Medium

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/glpi/ Parámetros: X-Frame-Options

2-http://172.21.5.250/glpi Parámetros: X-Frame-Options

Recomendación

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

Referencias

http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Exploración de Directorios

Descripción

Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc., que se pueden acceder para leer información sensible.

Riesgo

Medium

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/glpi/lib/tiny_mce/ Atacar: Parent Directory

2-http://172.21.5.250/glpi/lib/jqueryplugins/spectrum-colorpicker/ Atacar: Parent Directory

3-http://172.21.5.250/glpi/lib/jqueryplugins/select2/ Atacar: Parent Directory

4-http://172.21.5.250/glpi/lib/jqueryplugins/rateit/ Atacar: Parent Directory

5-http://172.21.5.250/glpi/lib/jqueryplugins/qtip2/ Atacar: Parent Directory

6-http://172.21.5.250/glpi/lib/jqueryplugins/jstree/ Atacar: Parent Directory

7-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-ui-timepicker-addon/i18n/ Atacar: Parent Directory

8-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-gantt/js/ Atacar: Parent Directory

9-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-gantt/css/ Atacar: Parent Directory

10-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-file-upload/js/ Atacar: Parent Directory

11-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-file-upload/ Atacar: Parent Directory

12-http://172.21.5.250/glpi/lib/jqueryplugins/jcrop/ Atacar: Parent Directory

13-http://172.21.5.250/glpi/lib/jqueryplugins/imagepaste/ Atacar: Parent Directory

14-http://172.21.5.250/glpi/lib/jqueryplugins/backtotop/ Atacar: Parent Directory

15-http://172.21.5.250/glpi/lib/jqueryplugins/autogrow/ Atacar: Parent Directory

16-http://172.21.5.250/glpi/lib/jqueryplugins/ Atacar: Parent Directory

17-http://172.21.5.250/glpi/lib/jquery/js/ Atacar: Parent Directory

18-http://172.21.5.250/glpi/lib/jquery/i18n/ Atacar: Parent Directory

19-http://172.21.5.250/glpi/lib/jquery/css/smoothness/ Atacar: Parent Directory

20-http://172.21.5.250/glpi/lib/jquery/css/ Atacar: Parent Directory

21-http://172.21.5.250/glpi/lib/jquery/ Atacar: Parent Directory

22-http://172.21.5.250/glpi/css/palettes/ Atacar: Parent Directory

23-http://172.21.5.250/glpi/css/jstree/ Atacar: Parent Directory

24-http://172.21.5.250/glpi/css/ Atacar: Parent Directory

Recomendación

Desactivar la exploración de directorios. Si esto es necesario, asegúrese de que los archivos de la lista no inducen riesgos.

Referencias

http://httpd.apache.org/docs/mod/core.html#options

http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html

X-Content-Type-Options Header Missing

Descripción

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Riesgo

Low

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/glpi/script.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

2-http://172.21.5.250/glpi/lib/tiny_mce/tiny_mce.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

3-http://172.21.5.250/glpi/lib/jqueryplugins/spectrum-colorpicker/spectrum.css
Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

4-http://172.21.5.250/glpi/lib/jqueryplugins/spectrum-colorpicker/spectrum-min.js
Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

5-http://172.21.5.250/glpi/lib/jqueryplugins/select2/select2_locale_es.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

6-http://172.21.5.250/glpi/lib/jqueryplugins/select2/select2.min.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

7-http://172.21.5.250/glpi/lib/jqueryplugins/select2/select2.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

8-http://172.21.5.250/glpi/lib/jqueryplugins/rateit/rateit.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

9-http://172.21.5.250/glpi/lib/jqueryplugins/rateit/jquery.rateit.min.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

10-http://172.21.5.250/glpi/lib/jqueryplugins/qtip2/jquery.qtip.min.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

11-http://172.21.5.250/glpi/lib/jqueryplugins/qtip2/jquery.qtip.min.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

12-http://172.21.5.250/glpi/lib/jqueryplugins/jstree/jquery.jstree.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

13-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-ui-timepicker-addon/jquery-ui-timepicker-addon.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

14-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-ui-timepicker-addon/i18n/jquery-ui-timepicker-es.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

15-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-gantt/js/jquery.fn.gantt.min.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

16-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-gantt/css/style.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

17-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-file-upload/js/jquery.iframe-transport.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

18-http://172.21.5.250/glpi/lib/jqueryplugins/jquery-file-upload/js/jquery.fileupload.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

19-http://172.21.5.250/glpi/lib/jqueryplugins/jcrop/jquery.Jcrop.min.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

20-http://172.21.5.250/glpi/lib/jqueryplugins/jcrop/jquery.Jcrop.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

21-http://172.21.5.250/glpi/lib/jqueryplugins/imagepaste/jquery.image_paste.js
Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

22-http://172.21.5.250/glpi/lib/jqueryplugins/backtotop/BackToTop.min.jquery.js
Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

23-http://172.21.5.250/glpi/lib/jqueryplugins/autogrow/jquery.autogrow-textarea.js

Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

24-http://172.21.5.250/glpi/lib/jquery/js/jquery-ui-1.10.4.custom.min.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

25-http://172.21.5.250/glpi/lib/jquery/js/jquery-1.10.2.min.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

26-http://172.21.5.250/glpi/lib/jquery/i18n/jquery.ui.datepicker-es.js Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

27-http://172.21.5.250/glpi/lib/jquery/css/smoothness/jquery-ui-1.10.4.custom.min.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

28-http://172.21.5.250/glpi/front/lostpassword.php?lostpassword=1 Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

29-http://172.21.5.250/glpi/front/lostpassword.php Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

30-http://172.21.5.250/glpi/front/login.php Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

31-http://172.21.5.250/glpi/css/styles_ie.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

32-http://172.21.5.250/glpi/css/styles.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

33-http://172.21.5.250/glpi/css/print.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

34-http://172.21.5.250/glpi/css/palettes/auror.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

35-http://172.21.5.250/glpi/css/jstree/style.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still

Affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

36-http://172.21.5.250/glpi/css/jquery-glpi.css Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

37-http://172.21.5.250/glpi/ Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

38-http://172.21.5.250/glpi Parámetros: X-Content-Type-Options

Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

Recomendación

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Referencias

http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Web Browser XSS Protection Not Enabled

Descripción

Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Riesgo

Low

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/sitemap.xml Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

2-http://172.21.5.250/robots.txt Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

3-http://172.21.5.250/glpi/front/lostpassword.php?lostpassword=1 Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the

Web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

4-http://172.21.5.250/glpi/front/lostpassword.php Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

5-http://172.21.5.250/glpi/front/login.php Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

6-http://172.21.5.250/glpi/ Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

7-http://172.21.5.250/glpi Parámetros: X-XSS-Protection

Otra información: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss the following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

Recomendación

Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

Referencias

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/

Password Autocomplete in Browser

Descripción

The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.

Riesgo

Low

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/glpi/ Parámetros: login password

Evidencia: <input type="password" name="login_password" id="login_password" required="required" placeholder="Contraseña" />

2-http://172.21.5.250/glpi Parámetros: login_password

Evidencia: <input type="password" name="login_password" id="login_password" required="required" placeholder="Contraseña" />

Recomendación

Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.

Referencias

http://www.w3schools.com/tags/att_input_autocomplete.asp

https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx

Cookie No HttpOnly Flag

Descripción

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Riesgo

Low

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/glpi/front/lostpassword.php?lostpassword=1
Parámetros: glpi_3f946f74140a3178722cb675d5bf6b47
Evidencia: Set-Cookie: glpi_3f946f74140a3178722cb675d5bf6b47

2-http://172.21.5.250/glpi/front/lostpassword.php
Parámetros: glpi_3f946f74140a3178722cb675d5bf6b47
Evidencia: Set-Cookie: glpi_3f946f74140a3178722cb675d5bf6b47

3-http://172.21.5.250/glpi/front/login.php

Parámetros: glpi_3f946f74140a3178722cb675d5bf6b47

Evidencia: Set-Cookie: glpi_3f946f74140a3178722cb675d5bf6b47

4-http://172.21.5.250/glpi/

Parámetros: glpi_3f946f74140a3178722cb675d5bf6b47

Evidencia: Set-Cookie: glpi_3f946f74140a3178722cb675d5bf6b47

5-http://172.21.5.250/glpi

Parámetros: glpi_3f946f74140a3178722cb675d5bf6b47

Evidencia: Set-Cookie: glpi_3f946f74140a3178722cb675d5bf6b47

Recomendación

Ensure that the HttpOnly flag is set for all cookies.

Referencias

http://www.owasp.org/index.php/HttpOnly

Private IP Disclosure

Descripción

A private IP such as 10.x.x.x, 172.x.x.x, 192.168.x.x has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

Riesgo

Low

Confiabilidad

Medium

URLs vulnerables

1-http://172.21.5.250/sitemap.xml Evidencia: 172.21.5.250
Otra información: 172.21.5.250

2-http://172.21.5.250/robots.txt Evidencia: 172.21.5.250

Otra información: 172.21.5.250

3-http://172.21.5.250/glpi Evidencia: 172.21.5.250

Otra información: 172.21.5.250 172.21.5.250

Recomendación

Remove the private IP address from the HTTP response body. For comments, use JSP/ASP comment instead of HTML/JavaScript comment which can be seen by client browsers.

Referencias

https://tools.ietf.org/html/rfc1918

Anexo E. Lista de riesgos de seguridad

Dueño /responsable	Categoría	Tipo (primario - soporte)	Nombre Activo	Disponibilidad	Integridad	Confidencialidad	Impacto	Vulnerabilidades	Amenazas
Carlos Neuto	Hardware	Soporte	Caja fuerte	4	4	4	4	Almacenamiento sin protección	Hurto o perdida
Heriberto Ceballos		Soporte	Impresoras	3	3	2	2	Almacenamiento sin protección	Manipulación de la información
Heriberto Ceballos		Soporte	Access point	4	4	3	3	Ausencia de un eficiente control de cambios en la configuración	Explotación de configuraciones por defecto
Heriberto Ceballos		Soporte	Ups	4	4	3	4	Ausencia de un eficiente control de cambios en la configuración	Daño por agua
Heriberto Ceballos		Soporte	Servidor de aplicaciones	4	4	3	4		Negación de servicio
Rafael Palacino		Soporte	Teléfono celular	3	3	2	2		Uso inadecuado del equipo
Heriberto Ceballos		Soporte	Sistema de vacuo	4	4	4	5	Copia no controlada	Falla en el sistema
Heriberto Ceballos		Soporte	Disco duro para backup	4	4	4	5		
Heriberto Ceballos		Soporte	DVR	4	4	4	4		Hurto de medios
Heriberto Ceballos		Soporte	Teléfonos celulares	3	3	2	2	Falta de cuidado en la disposición final	Hurto de información
Rafael Palacino		Soporte	Camioneta	3	3	2	3	Falta de seguimiento satelital	
Rafael Palacino		Soporte	Moto	3	3	2	3		Hurto o perdida por delincuencia en la ciudad
Heriberto Ceballos		Soporte	Servidor de archivos	4	4	3	4	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
Carlos Neuto		Soporte	Computadores del área financiera	3	4	4	3	Susceptibilidad a la humedad, el polvo y la suciedad	Falla en el sistema
Heriberto Ceballos		Soporte	Planta telefónica	4	4	3	3		Mal funcionamiento
Rafael Palacino		Soporte	Computadores del área logística	3	4	3	3		Perdida de información
Carlos Neuto		Soporte	Token banco	4	5	5	5		Uno no autorizado
Rafael Palacino		Soporte	Sistema de vigilancia	4	4	2	3	Susceptibilidad a las variaciones de voltaje	Polvo o corrosión
Heriberto Ceballos		Soporte	Switches	4	4	3	3		
Heriberto Ceballos		Soporte	Router	4	4	3	3		
Heriberto Ceballos		Soporte	Parque informático	4	4	3	3		Uso inadecuado del equipo
Carlos Neuto	Lugar	Soporte	Oficinas administrativas	4	4	3	3	Ausencia de protección física de la edificación, puertas y ventanas	Fenómenos climáticos
Rafael Palacino		Soporte	Bodega de almacenamiento	4	4	4	4		Inundación
Heriberto Ceballos		Soporte	Cuarto de comunicaciones	4	4	4	4		Hurto
Heriberto Ceballos		Soporte	Cuarto de servicio técnico	4	4	2	3	Red energética inestable	Perdida del suministro de energía
Rafael Palacino	Organización	Primario	Informes del área logística	3	4	3	3	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado
Rafael Palacino		Primario	Contratos de servicios	4	4	4	5	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	
Rafael Palacino		Primario	Factura de proveedor	3	4	2	3		Manipulación de la información
Rafael Palacino		Primario	Documentos de garantías	4	4	3	4		Hurto de medios o documentos
Rafael Palacino		Primario	Pedidos de compra	3	4	4	3		
Rafael Palacino		Primario	Pedidos de venta	3	4	4	3		Incumplimiento de los acuerdos establecidos
Rafael Palacino		Primario	Procedimiento de garantías	3	4	2	3		Abuso de derechos
Marisol vela		Primario	Pago a proveedores	4	4	4	5	Ausencia de auditorías (supervisiones) regulares	Abuso de derechos
Carlos Neuto		Primario	Estados financieros	4	5	4	3		Procesamiento ilegal de datos
Carlos Neuto		Primario	Verificación de datos	4	4	4	3		Corrupción de datos
Carlos Neuto		Primario	Consignaciones	3	4	4	3		Abuso de derechos
Carlos Neuto		Primario	Conciliaciones bancarias	3	5	4	4		Manipulación de la información
Carlos Neuto		Primario	Comprobantes de nomina	3	5	5	3	Ausencia de la asignación adecuada de responsabilidades en la seguridad de la información	Uso no autorizado
Carlos Neuto		Primario	Inventario de activos fijos	3	5	3	3		Manipulación de la información
Carlos Neuto		Primario	Informes de revisoría fiscal	4	5	5	3	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
Heriberto Ceballos		Primario	Continuidad de negocio	4	5	5	5	Ausencia de planes de continuidad documentados	Negación de servicio
Carlos Neuto		Primario	Extractos bancarios	3	5	4	3	Ausencia de políticas sobre el uso del correo electrónico	Manipulación de la información
Rafael Palacino		Primario	Órdenes de compra	3	4	3	3		
Rafael Palacino		Primario	Remisiones	2	3	3	4		Sabotaje
Carlos Neuto		Primario	Impuestos	4	5	4	4	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Falla en el sistema
Carlos Neuto		Primario	Informes financieros	4	5	4	4	Ausencia de procedimiento formal para el control de la documentación del SGSI	Manipulación de la información
Heriberto Ceballos		Primario	Creación de credenciales (ad, correo, ERP)	3	3	4	3	Ausencia de procedimiento formal para el registro y retiro de usuarios	Instrucción con credenciales de usuarios retirados
Carlos Neuto		Primario	Legalización de gastos	3	4	3	3	Ausencia de procedimiento formal para la autorización de la información disponible al publico	Manipulación de la información
Heriberto Ceballos		Primario	Manuales de usuario	4	3	2	3		Perdida de información
Marisol vela		Primario	Creación de cuentas contables	3	5	3	3	Ausencia de procedimiento formal para la revisión (supervisión) de los derechos de acceso	Falla en el sistema

Dueño /responsable	Categoría	Tipo (primario - soporte)	Nombre Activo	Disponibilidad	Integridad	Confidencialidad	Impacto	Vulnerabilidades	Amenazas
Carlos Neuto		Primario	Anticipos	2	4	2	2	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Manipulación de la información
Heriberto Ceballos		Primario	Inventario de activos tecnológicos	2	4	4	3		Manipulación de la información
Heriberto Ceballos		Primario	Planos del edificio	3	3	2	2	Ausencia de procedimientos de control de cambios	Hurto de medios o documentos
Heriberto Ceballos		Primario	Indicadores de medición de IT	3	3	3	3		Sabotaje
Carlos Neuto		Primario	Custodia de bienes	4	5	4	3	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de derechos
Rafael Palacino		Primario	Factura de cliente	3	4	2	3	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Perdida de medios
Carlos Neuto		Primario	Parafiscales	3	4	3	3	Ausencia de procedimientos disciplinarios definidos en el caso de incidentes de seguridad de la información	Manipulación de información
Carlos Neuto		Primario	Indicadores de medición	3	5	4	3		Sabotaje
Carlos Neuto		Primario	Registro de proveedores	3	4	3	3	Ausencia de procedimientos para el manejo de información clasificada	Manipulación de la información
Carlos Neuto		Primario	Registro de clientes	3	4	3	3		
Rafael Palacino		Primario	Registros de correspondencia	3	3	3	2		
Rafael Palacino		Primario	Reporte de ventas	3	4	3	3		
Rafael Palacino		Primario	Actas del comité de compras	2	3	3	2		
Rafael Palacino		Primario	Comprobantes de devolución de mercancía	2	4	3	3		Perdida de medios
Rafael Palacino		Primario	Comprobantes de entrada por devolución	2	4	3	3		
Rafael Palacino		Primario	Comprobantes de recibo de mercancía	2	4	3	4		
Heriberto Ceballos		Primario	Diagrama de red	3	4	4	3		Error en el uso
Heriberto Ceballos		Primario	Diagrama de datacenter	3	4	4	3		
Heriberto Ceballos		Primario	Documentación de sistemas de información	3	3	3	3		
Heriberto Ceballos		Primario	Inventario de sistemas de información	3	3	3	2		Manipulación de la información
Heriberto Ceballos		Primario	Inventario de sistemas de información críticos	3	3	3	3		
Carlos Neuto		Primario	Información financiera de clientes	3	4	5	4	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Uso no autorizado
Carlos Neuto		Primario	Documentos para el estudio de crédito	3	4	5	3	Ausencia de registros en las bitácoras (logs) de administrador y operario	Perdida de información
Rafael Palacino		Primario	Planilla de recorrido diario - ruta	3	3	3	4		Error en el uso
Rafael Palacino		Primario	Inventario de vehículos	2	3	2	2		Uso inadecuado
Carlos Neuto		Primario	Comprobantes de causación	4	5	4	4	Ausencia de reportes de fallas en los registros de administradores y operadores	Manipulación de la información
Rafael Palacino		Primario	Directorio telefónico de clientes y proveedores	4	4	2	3	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Uso no autorizado
Carlos Neuto		Primario	Cuentas por pagar	3	4	4	4	Ausencia de revisiones regulares por parte de la gerencia	Manipulación de la información
Carlos Neuto		Primario	Cuentas por cobrar	3	4	4	3		
Carlos Neuto		Primario	Contratos	3	5	4	4	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con clientes o terceras partes	Perdida de medios
Carlos Neuto		Soporte	Backup de archivos financiera	4	5	4	3	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Perdida de información
Carlos Neuto		Primario	Registro de aportes sociales	3	4	3	3	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Manipulación de la información
Marisol vela	Persona	Primario	Empleados	4	4	4	5	Falta de conciencia acerca de la seguridad	Ingeniería social
Rafael Palacino		Soporte	Personal de mensajería	4	4	3	5	Entrenamiento insuficiente en seguridad	Ingeniería social
Heriberto Ceballos		Soporte	Ingenieros de soporte	4	4	3	5	Uso incorrecto de hardware y software	Uso inadecuado del equipo
Heriberto Ceballos		Soporte	Ingenieros de soporte	4	4	3	5	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Perdida de información
Heriberto Ceballos		Soporte	Personal de outsourcing técnico	4	4	3	5	Procedimiento inadecuado de contratación	Abuso de derechos
Heriberto Ceballos		Soporte	Personal de outsourcing técnico	4	4	3	5	Ausencia de mecanismos de monitoreo	Destrucción de equipos o medios
Heriberto Ceballos		Soporte	Personal de outsourcing técnico	4	4	3	5	Ausencia de personal	Ausencia y/o no disponibilidad del personal
Marisol vela	Red	Soporte	Internet - portal de bancos	4	4	5	3	Ausencia de pruebas de envío o recepción de paquetes punto único de falla	Falla en el equipo de comunicaciones (ISP)
Carlos Neuto		Primario	Carpeta compartida financiera	3	5	4	3		Perdida de información
Carlos Neuto		Soporte	Servicio de telefonía	4	3	3	3		Falla en el equipo de comunicaciones (ISP)
Carlos Neuto		Soporte	Servicio de internet	4	4	4	3		Falla en el equipo de comunicaciones (ISP)
Carlos Neuto		Soporte	Red de datos	5	4	4	3		Falla en el equipo centralizado de enrutamiento
Rafael Palacino		Soporte	Servicio de telefonía	3	4	2	3		Falla en el equipo de comunicaciones (ISP)
Heriberto Ceballos		Soporte	Red de datos	5	4	2	3		Falla en el equipo centralizado de enrutamiento
Heriberto Ceballos		Soporte	CCTV	5	4	3	3		Fallas en el DVR o cámaras
Heriberto Ceballos		Soporte	Servicio de correo electrónico	4	4	3	3		Falla del sistema

Dueño /responsable	Categoría	Tipo (primario - soporte)	Nombre Activo	Disponibilidad	Integridad	Confidencialidad	Impacto	Vulnerabilidades	Amenazas
Heriberto Ceballos		Soporte	Red wifi	3	3	2	2		Instrucción con credenciales de usuarios retirados
Heriberto Ceballos		Soporte	Internet	4	4	3	3		Falla en el equipo de comunicaciones (ISP)
Heriberto Ceballos		Soporte	Red de energía regulada	4	4	2	4		Mal funcionamiento
Carlos Neuto	Software	Soporte	Modulo financiero ERP world office	4	4	4	3	Asignación errada de los derechos de acceso	Falla en el sistema
Rafael Palacino		Soporte	Módulo de logística ERP worldoffice	4	4	3	3		Mal funcionamiento del software
Heriberto Ceballos		Primario	Base de datos directorio activo	3	4	4	3		Mal funcionamiento
Heriberto Ceballos		Soporte	ERP worldoffice	3	4	3	3		Falla en la copia de seguridad
Carlos Neuto		Soporte	Suite office	4	4	3	3	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo	Mal funcionamiento
Carlos Neuto		Soporte	Correo electrónico	3	5	5	3		Negación del servicio
Heriberto Ceballos		Soporte	Software de tickets	2	3	3	2		Falla en la copia de seguridad
Heriberto Ceballos		Primario	Página web	4	4	3	3		Negación del servicio
Rafael Palacino		Primario	Base de datos de clientes	3	4	4	4	Configuración incorrecta de parámetros	Manipulación con software
Heriberto Ceballos		Soporte	Consola de antivirus	3	4	3	3		Uso no autorizado
Heriberto Ceballos		Soporte	Software unifi	4	4	3	3		Falla en la copia de seguridad
Heriberto Ceballos		Soporte	Servidor virtual de tickets	4	4	3	3	Descarga y uso no controlado de software	Código malicioso
Rafael Palacino		Soporte	Suite office - Excel	2	3	2	3	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Falla en el sistema
Heriberto Ceballos		Primario	Código fuente de sistemas o desarrollos	3	3	3	3		Manipulación de la información
Heriberto Ceballos		Soporte	Hyper-v	3	4	3	3		Falla en el sistema
Rafael Palacino		Primario	Base de datos de proveedores	3	4	3	4	Falta de actualizaciones requeridas	Negación del servicio
Heriberto Ceballos		Primario	Base de datos ERP	4	4	4	4	Servicios innecesarios habilitados	Explotación de configuraciones por defecto

Anexo F. Evaluación de riesgos (Probabilidad / Impacto)

DUEÑO /RESPONSABLE	CATEGORÍA	TIPO (PRIMARIO - SOPORTE)	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO	VULNERABILIDADES	AMENAZAS	PROBABILIDAD DE OCURRENCIA	RIESGO
CARLOS NEUTO	HARDWARE	SOPORTE	CAJA FUERTE	4	4	4	4	ALMACENAMIENTO SIN PROTECCIÓN	HURTO O PERDIDA	2	8
HERIBERTO CEBALLOS		SOPORTE	IMPRESORAS	3	3	2	2	ALMACENAMIENTO SIN PROTECCIÓN	MANIPULACIÓN DE LA INFORMACIÓN	4	8
HERIBERTO CEBALLOS		SOPORTE	ACCESS POINT	4	4	3	3	AUSENCIA DE UN EFICIENTE CONTROL DE CAMBIOS EN LA CONFIGURACIÓN	EXPLOTACIÓN DE CONFIGURACIONES POR DEFECTO	3	9
HERIBERTO CEBALLOS		SOPORTE	UPS	4	4	3	4	AUSENCIA DE UN EFICIENTE CONTROL DE CAMBIOS EN LA CONFIGURACIÓN	DAÑO POR AGUA	3	12
HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE APLICACIONES	4	4	3	4		NEGACIÓN DE SERVICIO	2	8
RAFAEL PALACINO		SOPORTE	TELÉFONO CELULAR	3	3	2	2		USO INADECUADO DEL EQUIPO	4	8
HERIBERTO CEBALLOS		SOPORTE	SISTEMA DE BAKCUP	4	4	4	5	COPIA NO CONTROLADA	FALLA EN EL SISTEMA	3	15
HERIBERTO CEBALLOS		SOPORTE	DISCO DURO PARA BACKUP	4	4	4	5			4	20
HERIBERTO CEBALLOS		SOPORTE	DVR	4	4	4	4		HURTO DE MEDIOS	4	16
HERIBERTO CEBALLOS		SOPORTE	TELÉFONOS CELULARES	3	3	2	2	FALTA DE CUIDADO EN LA DISPOSICIÓN FINAL	HURTO DE INFORMACIÓN	4	8
RAFAEL PALACINO		SOPORTE	CAMIONETA	3	3	2	3			3	9
RAFAEL PALACINO		SOPORTE	MOTO	3	3	2	3	FALTA DE SEGUIMIENTO SATELITAL	HURTO O PERDIDA POR DELINCUENCIA EN LA CIUDAD	3	9
HERIBERTO CEBALLOS		SOPORTE	SERVIDOR DE ARCHIVOS	4	4	3	4	HABILITACIÓN DE SERVICIOS INNECESARIOS	PROCESAMIENTO ILEGAL DE DATOS	3	12
CARLOS NEUTO		SOPORTE	COMPUTADORES DEL ÁREA FINANCIERA	3	4	4	3		FALLA EN EL SISTEMA	2	6
HERIBERTO CEBALLOS		SOPORTE	PLANTA TELEFÓNICA	4	4	3	3	SUSCEPTIBILIDAD A LA HUMEDAD, EL POLVO Y LA SUCIEDAD	MAL FUNCIONAMIENTO	4	12
RAFAEL PALACINO		SOPORTE	COMPUTADORES DEL ÁREA LOGÍSTICA	3	4	3	3		PERDIDA DE INFORMACIÓN	2	6
CARLOS NEUTO		SOPORTE	TOKEN BANCO	4	5	5	5		UNO NO AUTORIZADO	2	10
RAFAEL PALACINO		SOPORTE	SISTEMA DE VIGILANCIA	4	4	2	3	SUSCEPTIBILIDAD A LAS VARIACIONES DE VOLTAJE	POLVO O CORROSIÓN	4	12
HERIBERTO CEBALLOS		SOPORTE	SWITCHES	4	4	3	3			4	12
HERIBERTO CEBALLOS		SOPORTE	ROUTER	4	4	3	3			4	12
HERIBERTO CEBALLOS		SOPORTE	PARQUE INFORMÁTICO	4	4	3	3		USO INADECUADO DEL EQUIPO	3	9
CARLOS NEUTO	LUGAR	SOPORTE	OFICINAS ADMINISTRATIVAS	4	4	3	3	AUSENCIA DE PROTECCIÓN FÍSICA DE LA EDIFICACIÓN, PUERTAS Y VENTANAS	FENÓMENOS CLIMÁTICOS	2	6
RAFAEL PALACINO		SOPORTE	BODEGA DE ALMACENAMIENTO	4	4	4	4		INUNDACIÓN	3	12
HERIBERTO CEBALLOS		SOPORTE	CUARTO DE COMUNICACIONES	4	4	4	4		HURTO	4	16
HERIBERTO CEBALLOS		SOPORTE	CUARTO DE SERVICIO TÉCNICO	4	4	2	3	RED ENERGÉTICA INESTABLE	PERDIDA DEL SUMINISTRO DE ENERGÍA	3	9
RAFAEL PALACINO	ORGANIZACIÓN	PRIMARIO	INFORMES DEL ÁREA LOGÍSTICA	3	4	3	3	AUSENCIA DE PROCEDIMIENTOS PARA LA PRESENTACIÓN DE INFORMES SOBRE LAS DEBILIDADES EN LA SEGURIDAD	USO NO AUTORIZADO	3	9
RAFAEL PALACINO		PRIMARIO	CONTRATOS DE SERVICIOS	4	4	4	5	AUSENCIA DE ACUERDOS DE NIVEL DE SERVICIO O INSUFICIENCIA DE LOS MISMOS		3	15
RAFAEL PALACINO		PRIMARIO	FACTURA DE PROVEEDOR	3	4	2	3		MANIPULACIÓN DE LA INFORMACIÓN	3	9
RAFAEL PALACINO		PRIMARIO	DOCUMENTOS DE GARANTÍAS	4	4	3	4		HURTO DE MEDIOS O DOCUMENTOS	2	8
RAFAEL PALACINO		PRIMARIO	PEDIDOS DE COMPRA	3	4	4	3			2	6
RAFAEL PALACINO		PRIMARIO	PEDIDOS DE VENTA	3	4	4	3		INCUMPLIMIENTO DE LOS ACUERDOS ESTABLECIDOS	2	6

DUEÑO /RESPONSABLE	CATEGORÍA	TIPO (PRIMARIO - SOPORTE)	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO	VULNERABILIDADES	AMENAZAS	PROBABILIDAD DE OCURRENCIA	RIESGO
RAFAEL PALACINO		PRIMARIO	PROCEDIMIENTO DE GARANTÍAS	3	4	2	3		ABUSO DE DERECHOS	2	6
MARISOL VELA		PRIMARIO	PAGO A PROVEEDORES	4	4	4	5		ABUSO DE DERECHOS	2	10
CARLOS NEUTO		PRIMARIO	ESTADOS FINANCIEROS	4	5	4	3	AUSENCIA DE AUDITORIAS (SUPERVISIONES) REGULARES	PROCESAMIENTO ILEGAL DE DATOS	2	6
CARLOS NEUTO		PRIMARIO	VERIFICACIÓN DE DATOS	4	4	4	3		CORRUPCIÓN DE DATOS	2	6
CARLOS NEUTO		PRIMARIO	CONSIGNACIONES	3	4	4	3		ABUSO DE DERECHOS	3	9
CARLOS NEUTO		PRIMARIO	CONCILIACIONES BANCARIAS	3	5	4	4	AUSENCIA DE LA ASIGNACIÓN ADECUADA DE RESPONSABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN	MANIPULACIÓN DE LA INFORMACIÓN	2	8
CARLOS NEUTO		PRIMARIO	COMPROBANTES DE NOMINA	3	5	5	3		USO NO AUTORIZADO	2	6
CARLOS NEUTO		PRIMARIO	INVENTARIO DE ACTIVOS FIJOS	3	5	3	3		MANIPULACIÓN DE LA INFORMACIÓN	2	6
CARLOS NEUTO		PRIMARIO	INFORMES DE REVISORÍA FISCAL	4	5	5	3	AUSENCIA DE MECANISMOS DE MONITOREO ESTABLECIDOS PARA LAS BRECHAS EN LA SEGURIDAD	HURTO DE MEDIOS O DOCUMENTOS	2	6
HERIBERTO CEBALLOS		PRIMARIO	CONTINUIDAD DE NEGOCIO	4	5	5	5	AUSENCIA DE PLANES DE CONTINUIDAD DOCUMENTADOS	NEGACIÓN DE SERVICIO	3	15
CARLOS NEUTO		PRIMARIO	EXTRACTOS BANCARIOS	3	5	4	3			2	6
RAFAEL PALACINO		PRIMARIO	ORDENES DE COMPRA	3	4	3	3	AUSENCIA DE POLÍTICAS SOBRE EL USO DEL CORREO ELECTRÓNICO	MANIPULACIÓN DE LA INFORMACIÓN	3	9
RAFAEL PALACINO		PRIMARIO	REMISIONES	2	3	3	4		SABOTAJE	2	8
CARLOS NEUTO		PRIMARIO	IMPUESTOS	4	5	4	4	AUSENCIA DE PROCEDIMIENTO DE MONITOREO DE LOS RECURSOS DE PROCESAMIENTO DE INFORMACIÓN	FALLA EN EL SISTEMA	2	8
CARLOS NEUTO		PRIMARIO	INFORMES FINANCIEROS	4	5	4	4	AUSENCIA DE PROCEDIMIENTO FORMAL PARA EL CONTROL DE LA DOCUMENTACIÓN DEL SGSI	MANIPULACIÓN DE LA INFORMACIÓN	2	8
HERIBERTO CEBALLOS		PRIMARIO	CREACIÓN DE CREDENCIALES (AD, CORREO, ERP)	3	3	4	3	AUSENCIA DE PROCEDIMIENTO FORMAL PARA EL REGISTRO Y RETIRO DE USUARIOS	INSTRUCCIÓN CON CREDENCIALES DE USUARIOS RETIRADOS	4	12
CARLOS NEUTO		PRIMARIO	LEGALIZACIÓN DE GASTOS	3	4	3	3	AUSENCIA DE PROCEDIMIENTO FORMAL PARA LA AUTORIZACIÓN DE LA INFORMACIÓN DISPONIBLE AL PUBLICO	MANIPULACIÓN DE LA INFORMACIÓN	3	9
HERIBERTO CEBALLOS		PRIMARIO	MANUALES DE USUARIO	4	3	2	3		PERDIDA DE INFORMACIÓN	2	6
MARISOL VELA		PRIMARIO	CREACIÓN DE CUENTAS CONTABLES	3	5	3	3	AUSENCIA DE PROCEDIMIENTO FORMAL PARA LA REVISIÓN (SUPERVISIÓN) DE LOS DERECHOS DE ACCESO	FALLA EN EL SISTEMA	3	9
CARLOS NEUTO		PRIMARIO	ANTICIPOS	2	4	2	2	AUSENCIA DE PROCEDIMIENTO FORMAL PARA LA SUPERVISIÓN DEL REGISTRO DEL SGSI	MANIPULACIÓN DE LA INFORMACIÓN	2	4
HERIBERTO CEBALLOS		PRIMARIO	INVENTARIO DE ACTIVOS ETNOLÓGICOS	2	4	4	3		MANIPULACIÓN DE LA INFORMACIÓN	2	6
HERIBERTO CEBALLOS		PRIMARIO	PLANOS DEL EDIFICIO	3	3	2	2	AUSENCIA DE PROCEDIMIENTOS DE CONTROL DE CAMBIOS	HURTO DE MEDIOS O DOCUMENTOS	1	2
HERIBERTO CEBALLOS		PRIMARIO	INDICADORES DE MEDICIÓN DE IT	3	3	3	3		SABOTAJE	2	6
CARLOS NEUTO		PRIMARIO	CUSTODIA DE BIENES	4	5	4	3	AUSENCIA DE PROCEDIMIENTOS DE IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS	ABUSO DE DERECHOS	2	6
RAFAEL PALACINO		PRIMARIO	FACTURA DE CLIENTE	3	4	2	3	AUSENCIA DE PROCEDIMIENTOS DEL CUMPLIMIENTO DE LAS DISPOSICIONES CON LOS DERECHOS INTELECTUALES	PERDIDA DE MEDIOS	4	12
CARLOS NEUTO		PRIMARIO	PARAFISCALES	3	4	3	3	AUSENCIA DE PROCEDIMIENTOS DISCIPLINARIOS DEFINIDOS EN EL CASO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	MANIPULACIÓN DE INFORMACIÓN	2	6
CARLOS NEUTO		PRIMARIO	INDICADORES DE MEDICIÓN	3	5	4	3		SABOTAJE	2	6
CARLOS NEUTO		PRIMARIO	REGISTRO DE PROVEEDORES	3	4	3	3			3	9
CARLOS NEUTO		PRIMARIO	REGISTRO DE CLIENTES	3	4	3	3			3	9
RAFAEL PALACINO		PRIMARIO	REGISTROS DE CORRESPONDENCIA	3	3	3	2		MANIPULACIÓN DE LA INFORMACIÓN	3	6
RAFAEL PALACINO		PRIMARIO	REPORTE DE VENTAS	3	4	3	3			2	6
RAFAEL PALACINO		PRIMARIO	ACTAS DEL COMITÉ DE COMPRAS	2	3	3	2	AUSENCIA DE PROCEDIMIENTOS PARA EL MANEJO DE INFORMACIÓN CLASIFICADA		2	4
RAFAEL PALACINO		PRIMARIO	COMPROBANTES DE DEVOLUCIÓN DE MERCANCÍA	2	4	3	3			3	9
RAFAEL PALACINO		PRIMARIO	COMPROBANTES DE ENTRADA POR DEVOLUCIÓN	2	4	3	3		PERDIDA DE MEDIOS	3	9
RAFAEL PALACINO		PRIMARIO	COMPROBANTES DE RECIBO DE MERCANCÍA	2	4	3	4			3	12
HERIBERTO CEBALLOS		PRIMARIO	DIAGRAMA DE RED	3	4	4	3		ERROR EN EL USO	2	6

DUEÑO /RESPONSABLE	CATEGORÍA	TIPO (PRIMARIO - SOPORTE)	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO	VULNERABILIDADES	AMENAZAS	PROBABILIDAD DE OCURRENCIA	RIESGO
HERIBERTO CEBALLOS		PRIMARIO	DIAGRAMA DE DATACENTER	3	4	4	3			2	6
HERIBERTO CEBALLOS		PRIMARIO	DOCUMENTACIÓN DE SISTEMAS DE INFORMACIÓN	3	3	3	3			2	6
HERIBERTO CEBALLOS		PRIMARIO	INVENTARIO DE SISTEMAS DE INFORMACIÓN	3	3	3	2		MANIPULACIÓN DE LA INFORMACIÓN	2	4
HERIBERTO CEBALLOS		PRIMARIO	INVENTARIO DE SISTEMAS DE INFORMACIÓN CRÍTICOS	3	3	3	3			2	6
CARLOS NEUTO		PRIMARIO	INFORMACIÓN FINANCIERA DE CLIENTES	3	4	5	4	AUSENCIA DE PROCEDIMIENTOS PARA LA INTRODUCCIÓN DEL SOFTWARE EN LOS SISTEMAS OPERATIVOS	USO NO AUTORIZADO	3	12
CARLOS NEUTO		PRIMARIO	DOCUMENTOS PARA EL ESTUDIO DE CRÉDITO	3	4	5	3		PERDIDA DE INFORMACIÓN	2	6
RAFAEL PALACINO		PRIMARIO	PLANILLA DE RECORRIDO DIARIO - RUTA	3	3	3	4	AUSENCIA DE REGISTROS EN LAS BITÁCORAS (LOGS) DE ADMINISTRADOR Y OPERARIO	ERROR EN EL USO	3	12
RAFAEL PALACINO		PRIMARIO	INVENTARIO DE VEHÍCULOS	2	3	2	2		USO INADECUADO	2	4
CARLOS NEUTO		PRIMARIO	COMPROBANTES DE CAUSACIÓN	4	5	4	4	AUSENCIA DE REPORTES DE FALLAS EN LOS REGISTROS DE ADMINISTRADORES Y OPERADORES	MANIPULACIÓN DE LA INFORMACIÓN	2	8
RAFAEL PALACINO		PRIMARIO	DIRECTORIO TELEFÓNICO DE CLIENTES Y PROVEEDORES	4	4	2	3	AUSENCIA DE RESPONSABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN EN LA DESCRIPCIÓN DE LOS CARGOS	USO NO AUTORIZADO	3	9
CARLOS NEUTO		PRIMARIO	CUENTAS POR PAGAR	3	4	4	4	AUSENCIA DE REVISIONES REGULARES POR PARTE DE LA GERENCIA	MANIPULACIÓN DE LA INFORMACIÓN	2	8
CARLOS NEUTO		PRIMARIO	CUENTAS POR COBRAR	3	4	4	3			2	6
CARLOS NEUTO		PRIMARIO	CONTRATOS	3	5	4	4	AUSENCIA O INSUFICIENCIA DE DISPOSICIONES (CON RESPECTO A LA SEGURIDAD) EN LOS CONTRATOS CON CLIENTES O TERCERAS PARTES	PERDIDA DE MEDIOS	2	8
CARLOS NEUTO		SOPORTE	BACKUP DE ARCHIVOS FINANCIERA	4	5	4	3	AUSENCIA O INSUFICIENCIA DE POLÍTICA SOBRE LIMPIEZA DE ESCRITORIO Y DE PANTALLA	PERDIDA DE INFORMACIÓN	2	6
CARLOS NEUTO		PRIMARIO	REGISTRO DE APORTES SOCIALES	3	4	3	3	AUSENCIA O INSUFICIENCIA EN LAS DISPOSICIONES (CON RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN) EN LO CONTRATOS CON LOS EMPLEADOS	MANIPULACIÓN DE LA INFORMACIÓN	2	6
MARISOL VELA		PRIMARIO	EMPLEADOS	4	4	4	5	FALTA DE CONCIENCIA ACERCA DE LA SEGURIDAD	INGENIERÍA SOCIAL	4	20
RAFAEL PALACINO		SOPORTE	PERSONAL DE MENSAJERÍA	4	4	3	5	ENTRENAMIENTO INSUFICIENTE EN SEGURIDAD	INGENIERÍA SOCIAL	4	20
HERIBERTO CEBALLOS		SOPORTE	INGENIEROS DE SOPORTE	4	4	3	5	USO INCORRECTO DE HARDWARE Y SOFTWARE	USO INADECUADO DEL EQUIPO	3	15
HERIBERTO CEBALLOS	PERSONA	SOPORTE	INGENIEROS DE SOPORTE	4	4	3	5	AUSENCIA DE POLÍTICAS PARA EL USO CORRECTO DE LOS MEDIOS DE TELECOMUNICACIONES Y MENSAJERÍA	PERDIDA DE INFORMACIÓN	3	15
HERIBERTO CEBALLOS		SOPORTE	PERSONAL DE OUTSOURCING TÉCNICO	4	4	3	5	PROCEDIMIENTO INADECUADO DE CONTRATACIÓN	ABUSO DE DERECHOS	3	15
HERIBERTO CEBALLOS		SOPORTE	PERSONAL DE OUTSOURCING TÉCNICO	4	4	3	5	AUSENCIA DE MECANISMOS DE MONITOREO	DESTRUCCIÓN DE EQUIPOS O MEDIOS	2	10
HERIBERTO CEBALLOS		SOPORTE	PERSONAL DE OUTSOURCING TÉCNICO	4	4	3	5	AUSENCIA DE PERSONAL	AUSENCIA Y/O NO DISPONIBILIDAD DEL PERSONAL	3	15
MARISOL VELA		SOPORTE	INTERNET - PORTAL DE BANCOS	4	4	5	3		FALLA EN EL EQUIPO DE COMUNICACIONES (ISP)	3	9
CARLOS NEUTO		PRIMARIO	CARPETA COMPARTIDA FINANCIERA	3	5	4	3		PERDIDA DE INFORMACIÓN	2	6
CARLOS NEUTO		SOPORTE	SERVICIO DE TELEFONÍA	4	3	3	3		FALLA EN EL EQUIPO DE COMUNICACIONES (ISP)	3	9
CARLOS NEUTO		SOPORTE	SERVICIO DE INTERNET	4	4	4	3		FALLA EN EL EQUIPO DE COMUNICACIONES (ISP)	3	9
CARLOS NEUTO		SOPORTE	RED DE DATOS	5	4	4	3		FALLA EN EL EQUIPO CENTRALIZADO DE ENRUTAMIENTO	3	9
RAFAEL PALACINO		SOPORTE	SERVICIO DE TELEFONÍA	3	4	2	3		FALLA EN EL EQUIPO DE COMUNICACIONES (ISP)	3	9
HERIBERTO CEBALLOS	RED	SOPORTE	RED DE DATOS	5	4	2	3	AUSENCIA DE PRUEBAS DE ENVÍO O RECEPCIÓN DE PAQUETES PUNTO ÚNICO DE FALLA	FALLA EN EL EQUIPO CENTRALIZADO DE ENRUTAMIENTO	3	9
HERIBERTO CEBALLOS		SOPORTE	CCTV	5	4	3	3		FALLAS EN EL DVR O CÁMARAS	2	6
HERIBERTO CEBALLOS		SOPORTE	SERVICIO DE CORREO ELECTRÓNICO	4	4	3	3		FALLA DEL SISTEMA	2	6
HERIBERTO CEBALLOS		SOPORTE	RED WIFI	3	3	2	2		INSTRUCCIÓN CON CREDENCIALES DE USUARIOS RETIRADOS	2	4
HERIBERTO CEBALLOS		SOPORTE	INTERNET	4	4	3	3		FALLA EN EL EQUIPO DE COMUNICACIONES (ISP)	3	9

DUEÑO /RESPONSABLE	CATEGORÍA	TIPO (PRIMARIO - SOPORTE)	NOMBRE ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO	VULNERABILIDADES	AMENAZAS	PROBABILIDAD DE OCURRENCIA	RIESGO
HERIBERTO CEBALLOS		SOPORTE	RED DE ENERGÍA REGULADA	4	4	2	4		MAL FUNCIONAMIENTO	3	12
CARLOS NEUTO	SOFTWARE	SOPORTE	MODULO FINANCIERO ERP WORLD OFFICE	4	4	4	3	ASIGNACIÓN ERRADA DE LOS DERECHOS DE ACCESO	FALLA EN EL SISTEMA	3	9
RAFAEL PALACINO		SOPORTE	MODULO DE LOGÍSTICA ERP WORLDOFFICE	4	4	3	3		MAL FUNCIONAMIENTO DEL SOFTWARE	3	9
HERIBERTO CEBALLOS		PRIMARIO	BASE DE DATOS DIRECTORIO ACTIVO	3	4	4	3		MAL FUNCIONAMIENTO	2	6
HERIBERTO CEBALLOS		SOPORTE	ERP WORLDOFFICE	3	4	3	3		FALLA EN LA COPIA DE SEGURIDAD	3	9
CARLOS NEUTO		SOPORTE	SUITE OFFICE	4	4	3	3	AUSENCIA DE TERMINACIÓN DE LA SESIÓN CUANDO SE ABANDONA LA ESTACIÓN DE TRABAJO	MAL FUNCIONAMIENTO	2	6
CARLOS NEUTO		SOPORTE	CORREO ELECTRÓNICO	3	5	5	3		NEGACIÓN DEL SERVICIO	2	6
HERIBERTO CEBALLOS		SOPORTE	SOFTWARE DE TICKETS	2	3	3	2		FALLA EN LA COPIA DE SEGURIDAD	3	6
HERIBERTO CEBALLOS		PRIMARIO	PAGINA WEB	4	4	3	3		NEGACIÓN DEL SERVICIO	2	6
RAFAEL PALACINO		PRIMARIO	BASE DE DATOS DE CLIENTES	3	4	4	4	CONFIGURACIÓN INCORRECTA DE PARÁMETROS	MANIPULACIÓN CON SOFTWARE	3	12
HERIBERTO CEBALLOS		SOPORTE	CONSOLA DE ANTIVIRUS	3	4	3	3		USO NO AUTORIZADO	2	6
HERIBERTO CEBALLOS		SOPORTE	SOFTWARE UNIFI	4	4	3	3		FALLA EN LA COPIA DE SEGURIDAD	3	9
HERIBERTO CEBALLOS		SOPORTE	SERVIDOR VIRTUAL DE TICKETS	4	4	3	3	DESCARGA Y USO NO CONTROLADO DE SOFTWARE	CODIGO MALICIOSO	4	12
RAFAEL PALACINO		SOPORTE	SUITE OFFICE - EXCEL	2	3	2	3		FALLA EN EL SISTEMA	3	9
HERIBERTO CEBALLOS		PRIMARIO	CODIGO FUENTE DE SISTEMAS O DESARROLLOS	3	3	3	3	DISPOSICIÓN O REUTILIZACIÓN DE LOS MEDIOS DE ALMACENAMIENTO SIN BORRADO ADECUADO	MANIPULACIÓN DE LA INFORMACIÓN	2	6
HERIBERTO CEBALLOS		SOPORTE	HYPER-V	3	4	3	3		FALLA EN EL SISTEMA	3	9
RAFAEL PALACINO		PRIMARIO	BASE DE DATOS DE PROVEEDORES	3	4	3	4	FALTA DE ACTUALIZACIONES REQUERIDAS	NEGACIÓN DEL SERVICIO	2	8
HERIBERTO CEBALLOS		PRIMARIO	BASE DE DATOS ERP	4	4	4	4	SERVICIOS INNECESARIOS HABILITADOS	EXPLOTACIÓN DE CONFIGURACIONES POR DEFECTO	2	8

Anexo G. Declaración de aplicabilidad

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
A.5	Políticas de Seguridad de la Información	A.5.1	Políticas de Seguridad de la Información: Proveen dirección y soporte acerca de cómo se debe ejecutar la seguridad de la información tomando en consideración los requerimientos del negocio y los elementos legales y regulatorios que son relevantes.	A.5.1.1 Política de Seguridad de la Información:	La organización debe tener políticas de seguridad de la información y la misma debe revisarse si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas. Debe ser publicada y comunicada a los empleados y a las partes externas relevantes.	S	N	Todos	
				A.5.1.2 Revisión de las Políticas de Seguridad de la Información:	Las políticas deben revisarse en intervalos planeados o si ocurriese algún cambio significativo, de tal forma que se asegure que siguen siendo funcionales, adecuadas y efectivas.	S	N	Todos	
A.6	Organización de la Seguridad de la Información	A.6.1	Organización de la seguridad de la información: Esta organización se requiere para establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la compañía	A.6.1.1 Roles y responsabilidades	Todas las responsabilidades relacionadas con la seguridad de la información, deben estar definidas y asignadas. Algunos ejemplos: Jefe de Seguridad de la Información, Dueño del Riesgo (Antes Dueño del Activo), Dueño del Proceso, entre otros.	S	N	Todos	
				A.6.1.2 - Segregación de funciones	Responsabilidades que están en conflicto a la hora de ejecutar un proceso (Por ejemplo ser juez y parte) y áreas de responsabilidad deben ser segregadas para reducir los riesgos identificados en nuestros procesos y las oportunidades de modificación y uso no apropiado de los activos de la organización.	S	S	Todos	
				A.6.1.3 - Contacto con autoridades	Se debe mantener un contacto apropiado con aquellas autoridades relevantes (internas o externas) que pudieran tener impacto o pudieran resultar impactadas por nuestros procesos.	S	N	Todos	
				A.6.1.4 - Contacto con grupos de interés especial	Se debe mantener un contacto apropiado con grupo de interés especial (internos o externos) que pudieran tener impacto o pudieran resultar impactados por nuestros procesos. Estos grupos incluyen foros especializados o asociaciones profesionales que tengan que ver con la seguridad de la información y/o con el manejo del riesgo en nuestros procesos y en	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
					nuestra organización.				
				A.6.1.5 - Seguridad de la información en la gestión de proyectos	Se debe mantener la seguridad de la información y el manejo adecuado del riesgo en la Gestión de Proyectos, sin importar la naturaleza o el tipo de proyecto.	S	N	Gestión de IT	
		A.6.2	Organización de la seguridad de la información: Asegurar la seguridad en el teletrabajo y uso de dispositivos móviles	A.6.2.1 Política para dispositivos móviles	Debe existir una política y medidas de seguridad que nos ayuden a gestionar los riesgos a los que nos podemos enfrentar ante el uso de dispositivos móviles.	S	N	Todos	
				A.6.2.2 Tele-trabajo (Teleworking)	Debe haber una política que nos ayude a proteger la información accesada, procesada o almacenada en los sitios donde se realiza tele-trabajo (Teleworking)	S	N	Todos	
A.7	Seguridad de los Recursos Humanos	A.7.1	Seguridad de los Recursos Humanos: Debemos asegurar que todos los empleados y personas contratadas entienden sus responsabilidades, y pueden asumir los roles para los cuales han sido considerados.	A.7.1.1 Revisión de antecedentes:	Se debe realizar la verificación y chequeo de los antecedentes de todos los candidatos a empleo; de acuerdo con la ley, regulaciones y de manera ética. La profundidad de esta verificación debe ir en proporción con los requerimientos y procesos de negocio en los cuales la persona tendrá inherencia, considerando como está clasificada la información a la que tendrá acceso y los riesgos percibidos y/o identificados en esos procesos.	S	N	RRHH	
				A.7.1.2 Términos y condiciones de empleo:	Los contratos de trabajo de los empleados y contratistas deben incluir sus responsabilidades en relación con la seguridad de la información al igual que las de la compañía.	S	N	RRHH	
		A.7.2	Seguridad de los Recursos Humanos: Debemos asegurar que todos los empleados y personas contratadas están conscientes y cumplen con sus responsabilidades relacionadas con la seguridad de la	A.7.2.1 Responsabilidades de la gerencia:	La gerencia debe requerir a todos los empleados y contratistas que cumplan con las políticas y procedimientos definidos para el manejo de la seguridad de la información. El no cumplimiento; puede originar una acción disciplinaria o la terminación de un contrato.	S	S	Todos	
				A.7.2.2 Concientización, educación y entrenamiento en	Todos los empleados de la organización y en las áreas donde sea relevante y los contratistas; deben recibir concientización, educación y entrenamiento sobre la seguridad	S	N	RRHH	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
			información.	seguridad de la información:	de la información. Asimismo y de manera regular, deben recibir actualizaciones acerca de las políticas y procedimientos relevantes con las funciones de su trabajo.				
				A.7.2.3 Proceso Disciplinario	Debe haber en vigencia un proceso disciplinario formal y comunicado. El mismo, debe contener los pasos a seguir en el caso de que algún empleado cometa alguna acción que va en contra de la seguridad de la información. Este mismo proceso debe hacerse extensivo a los contratistas cuando sea necesario.	S	N	RRHH	
		A.7.3	Seguridad de los Recursos Humanos: Debemos proteger los intereses de la organización como parte del proceso de cambio o terminación (desvinculación) de empleados.	A.7.3.1 Cambio en las responsabilidades laborales o terminación del contrato laboral	Este control tiene como propósito proteger los intereses de la organización cuando ocurre un cambio en las condiciones de empleo (Por ejemplo: Cambio de posición, funciones, etc.) o cuando termina el contrato de trabajo.	S	N	RRHH	
A.8	Gestión de Activos	A.8.1	Gestión de activos: Identificar los activos de la organización y definir las responsabilidades para protección apropiada	A.8.1.1 Inventario de activos	Debemos de identificar los activos asociados con los recursos de procesamiento de la información, adicional debemos establecer y mantener un inventario de estos activos.	S	S	Gestión de IT	
				A.8.1.2 Propiedad de los activos	Este control es aplicable debido a que todos los activos de información dentro del alcance deben estar inventariados y con un dueño asignado.	S	S	Todos	
				A.8.1.3 Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información, los activos asociados con la información y las instalaciones de procesamiento.	S	N	Todos	
				A.8.1.4 Retorno de activos	Todos los empleados y usuarios de terceras partes deben retornar los activos que tienen en su poder a la empresa luego de la terminación del contrato, acuerdo o desvinculación del empleado de la compañía.	S	S	RRHH	
		A.8.2	La gestión de activos:	A.8.2.1	La información se clasificará en términos de	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
			Para garantizar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.	Clasificación de la Información	requisitos legales, el valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.				
				A.8.2.2 Etiquetado de la información	Un conjunto apropiado de procedimientos para el etiquetado de información será elaborado y aplicado de acuerdo con el esquema de clasificación de la información adoptado por la organización.	S	N	Todos	
				A.8.2.3 Manejo de activos	Procedimientos para el manejo de los activos deberán ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la organización.	S	N	Todos	
		A.8.3	La gestión de activos: Para evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.	A.8.3.1 Gestión de medios extraíbles	Los procedimientos se aplicarán para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización.	S	N	Todos	
				A.8.3.2 Eliminación de los medios	Los medios de comunicación deberán ser desechados de manera segura cuando ya no sea necesario, utilizando procedimientos formales.	S	N	Todos	
				A.8.3.3 transferencia de medios físicos	Los medios que contienen información deberán estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante el transporte.	S	N	Todos	
A.9	Control de acceso	A.9.1	Control de acceso: Para limitar el acceso a las instalaciones de procesamiento de información y de información.	A.9.1.1 política de control de acceso	Se establecerá una política de control de acceso, documentado y revisado en base a los requisitos de seguridad y de información de negocios.	S	N	Gestión de IT	
				A.9.1.2 Acceso a redes y servicios en red	Los usuarios sólo deberán disponer de acceso a los servicios de red y a la red que han sido específicamente autorizados para su uso.	S	S	Gestión de IT	
		A.9.2	Control de acceso: Para garantizar el acceso de usuarios autorizados y para evitar el acceso no autorizado a los sistemas y servicios.	A.9.2.1 Registro y cancelación del registro de usuarios	Un proceso de registro de usuarios y cancelación de registro formal se llevará a cabo para permitir la asignación de derechos de acceso.	S	N	Gestión de IT	
				A.9.2.2 Suministro de acceso de usuarios	Un proceso formal de provisión de acceso de usuario deberá ser implementado para asignar o revocar los derechos de acceso para todo tipo de usuario a todos los sistemas y servicios.	S	N	Gestión de IT	
				A.9.2.3 Gestión de derechos de	La asignación y utilización de los derechos de acceso privilegiados serán restringidas y	S	S	Gestión de IT	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
				acceso privilegiado	controladas.				
				A.9.2.4 Gestión de información de autenticación secreta de los usuarios	La asignación de la información secreta de autenticación se controla a través de un proceso formal de gestión.	S	N	Gestión de IT	
				A.9.2.5 Revisión de los derechos de acceso de los usuarios	Los propietarios de activos deberán revisar los derechos de los usuarios a intervalos regulares.	S	S	Gestión de IT	
				A.9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y los usuarios externos a la información y las instalaciones de procesamiento de información deberán ser retirados después de la terminación de su empleo, contrato o acuerdo, o se deben ajustar cuando existan cambios.	S	S	Gestión de IT	
		A.9.3	Control de acceso: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.	A.9.3.1 Uso de la información de autenticación secreta	Los usuarios estarán obligados a seguir las prácticas de la organización en el uso de la información de autenticación secreta.	S	N	Gestión de IT	
		A.9.4	Control de acceso: Prevenir el acceso no autorizado a sistemas y aplicaciones.	A.9.4.1 restricción de acceso Información	El acceso a la información y a las funciones de los sistemas de aplicaciones se debe limitar de acuerdo con la política de control de acceso.	S	N	Gestión de IT	
				A.9.4.2 Procedimiento de inicio de sesión seguro	Cuando lo requiera la política de control de acceso, el acceso a los sistemas y aplicaciones se debe controlar mediante un procedimiento de conexión segura.	S	N	Gestión de IT	
				A.9.4.3 Sistema de gestión de contraseña	El sistema de gestión de claves de acceso debe ser interactivo y velar por la calidad de contraseña.	S	S	Gestión de IT	
				A.9.4.4 Uso de programas de utilidad privilegiados	El uso de programas de utilidades que podrían ser capaces de anular los controles del sistema y de las aplicaciones será restringido y estrechamente controlado.	S	N	Gestión de IT	
				A.9.4.5 Control de acceso al código fuente de programas	El acceso al código fuente de los programas deberá ser restringido.	S	S	Gestión de IT	
A.10	Criptografía	A.10.1	Criptografía: Para	Política A.10.1.1	Una política sobre el uso de controles	N	N	Gestión de IT	Sitech de

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
			garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.	en el uso de controles criptográficos	criptográficos para la protección de la información deberá ser desarrollada e implementada.				Colombia SA no implementara este control dado que toda la información confidencial o privilegiada del negocio se maneja en las aplicaciones centralizadas, a las cuales solo se accede por medios de comunicación seguros
				A.10.1.2 Gestión de llaves	Una política sobre el uso, la protección y la duración de las claves criptográficas se debe desarrollar e implementar en todo su ciclo de vida.	N	N	Gestión de IT	Sitech no implementa este control dado que ni usa Criptografía, este control no está en el alcance del SGSI
A.11	La seguridad física y ambiental	A.11.1	La seguridad física y ambiental: Prevenir el acceso físico no autorizado, daño e interferencia a la información y las instalaciones de procesamiento de información de la organización.	A.11.1.1 perímetro de seguridad física	Se deben definir y usar perímetros de seguridad para proteger áreas que contienen servicios de información y procesamiento de la información, ya sea sensibles o críticas.	S	N	Todos	
				A.11.1.2 Control de acceso Físico	Las áreas seguras deberán estar protegidas por controles de entrada adecuados para garantizar que sólo el personal autorizado se les permite el acceso.	S	N	RRHH	
				A.11.1.3 Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, recintos e instalaciones.	S	S	RRHH	
				A.11.1.4 Protección contra	La protección física contra los desastres naturales, ataques maliciosos o accidentes	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
				amenazas externas y ambientales	debe ser diseñada y aplicada.				
				A.11.1.5 Trabajo en áreas seguras	Procedimientos para trabajar en áreas seguras deberán ser diseñados y aplicados.	S	N	RRHH	
				A.11.1.6 áreas de entrega y carga	Los puntos de acceso, tales como áreas de entrega y de carga y otros puntos en los que personas no autorizadas puedan entrar en los locales se deberán controlar y, si es posible, aislada de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	S	S	Área Logística	
		A.11.2	La seguridad física y ambiental: Para evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.	A.11.2.1 Ubicación y protección de los equipos	Los equipos deberán estar ubicados y protegidas para reducir los riesgos de las amenazas ambientales o del entorno y los riesgos y las oportunidades de acceso no autorizado.	S	S	Todos	
				A.11.2.2 Servicios de suministro	Los equipos deberán estar protegidos contra fallos de alimentación de energía y otros trastornos causados por fallas en el apoyo a los servicios públicos.	S	N	Mantenimiento	
				A.11.2.3 Seguridad de cableado	El cableado de Energía y telecomunicaciones que transporta datos o apoya los servicios de información deberá estar protegido contra la interceptación, interferencia o daños.	S	S	Gestión de IT	
				A.11.2.4 Mantenimiento de equipos	Los Equipo deben mantenerse correctamente para asegurar su continua disponibilidad e integridad.	S	S	Gestión de IT	
				A.11.2.5 Retiro de activos	Equipos, información o software no se tendrán fuera de las instalaciones sin autorización previa.	S	S	RRHH	
				A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	S	S	Todos	
				A.11.2.7 Disposición segura o reutilización de los equipos	Todos los elementos de equipo que contienen medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y software con licencia han sido eliminados o sobrescritos de forma segura antes de su eliminación o reutilización.	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
				A.11.2.8 Equipo de usuario desatendido	Los usuarios deben asegurarse de que los equipos desatendidos tienen la protección adecuada.	S		Todos	
				A.11.2.9 Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento extraíbles y una política de pantalla limpia para las instalaciones de procesamiento de información.	S	N	Todos	
A.12	seguridad de las operaciones	A.12.1	Seguridad de las operaciones: Para garantizar operaciones correctas y seguras de instalaciones de procesamiento de información.	A.12.1.1 Procedimientos de operación documentados	Los procedimientos de operación deberán ser documentados y puestos a disposición de todos los usuarios que lo necesiten.	S	N	Todos	
				A.12.1.2 Gestión de cambios	Los cambios en la organización, los procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controladas.	S	N	Todos	
				A.12.1.3 Gestión de capacidad	Se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema	S	N	Gestión de IT	
				A.12.1.4 Separación de loa ambiente de desarrollo, prueba y producción	Los entornos de desarrollo, pruebas y operación se deben separar para reducir los riesgos de acceso o cambios no autorizados en el entorno de producción	S	N	Gestión de IT	
		A.12.2	Seguridad de las operaciones: Para asegurar que las instalaciones de procesamiento de información y la información están protegidos contra el malware.	A.12.2.1 Controles contra código malicioso	Se deben implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra código malicioso.	S	S	Gestión de IT	
		A.12.3	Copia de respaldo: Para evitar la pérdida de datos.	A.12.3.1 Respaldo de Información	Se deben realizar copias de seguridad de la información, software e imágenes de los sistemas y ponerlas a prueba periódicamente de acuerdo con una política de copia de seguridad acordada.	S	N	Gestión de IT	
		A.12.4	Registro y seguimiento:	A.12.4.1 registro	Se deben elaborar, conservar y revisar	S	N	Gestión de IT	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
			Registrar eventos y generar evidencia.	de eventos	regularmente los registros de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.				
				A.12.4.2 Protección de la información de registro	Registro de instalaciones y la información de registro se deben proteger contra la manipulación y acceso no autorizado.	S	N	Gestión de IT	
				A.12.4.3 Registros de administrador y del operador	Las actividades del administrador y del operador del sistema deberán ser registradas y sus registros protegidos y revisados con regularidad.	S	N	Gestión de IT	
				A.12.4.4 Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad deberán estar sincronizados a una sola fuente de referencia de tiempo.	S	S	Gestión de IT	
		A.12.5	Control de software operacional: Para garantizar la integridad de los sistemas operativos.	A.12.5.1 Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.	S	N	Gestión de IT	
		A.12.6	Gestión de Vulnerabilidad Técnica: Para evitar la explotación de las vulnerabilidades técnicas.	A.12.6.1 Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.	S	N	Gestión de IT	
				A.12.6.2 Restricciones sobre la instalación del software	Se establecerán y aplicarán normas que rigen la instalación de software por parte de los usuarios.	S	N	Gestión de IT	
		A.12.7	Consideraciones sobre auditorias de sistemas de información: Para minimizar el impacto de las actividades de auditoría en los sistemas operativos.	A.12.7.1 Controles de auditoría de sistemas Información	Los requisitos y las actividades de auditoria relacionadas con la verificación de los sistemas operativos deberán ser cuidadosamente planificados y acordados para minimizar las interrupciones a los procesos de negocio.	S	N	Gestión de IT, Gestión Financiera	
A.13	seguridad de las comunicaciones	A.13.1	Gestión de la seguridad de las redes: Para garantizar la protección	A.13.1.1 Controles de redes	La red será gestionada y controlada para proteger la información en los sistemas y aplicaciones.	S	S	Gestión de IT	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
			de la información en redes y sus instalaciones de apoyo de procesamiento de información.	A.13.1.2 Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red y se deben incluir en los acuerdos de servicios de red, si estos servicios se ofrecen en la empresa o es subcontratado.	S	N	Gestión de IT	
				A.13.1.3 Separación en las redes	Los grupos de servicios de información, los usuarios y los sistemas de información se deben separar en las redes.	S	N	Gestión de IT	
		A.13.2	Transferencia de Información: Para mantener la seguridad de la información transferida de una organización y con cualquier entidad externa.	A.13.2.1 Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	S	N	Todos	
				A.13.2.2 Acuerdos sobre transferencia de información	Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y las partes externas.	S	N	Todos	
				A.13.2.3 Mensajería electrónica	La Información involucrada en la mensajería electrónica deberá estar adecuadamente protegidos.	S	N	Gestión de IT	
				A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información.	S	N	Todos	
A.14	Adquisición, desarrollo y mantenimiento de sistemas	A.14.1	Análisis y especificación de requisitos de seguridad de la información: Para asegurarse de que la seguridad de la información es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.	A.14.1.1Analisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con la seguridad de la información se deben incluir en los requisitos para los nuevos sistemas de información o para mejoras a los sistemas de información existentes.	S	N	Todos	
				A.14.1.2 Protección de servicios de aplicaciones en redes públicas	La información que requiera servicios de aplicaciones que pasan a través de redes públicas deberá ser protegida contra la actividad fraudulenta, disputa contractual y la divulgación no autorizada y la modificación.	S	N	Gestión de IT	
				A.14.1.3 Protección de transacciones de servicios de aplicaciones	Información involucrada en las transacciones de los servicios de las aplicaciones debe ser protegido para evitar la transmisión incompleta, mal enrutamiento, alteración mensaje no autorizado, la divulgación no autorizada, la duplicación no autorizada o bien	S	N	Gestión de IT	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
					la repetición de mensajes.				
		A.14.2	Seguridad en los procesos de desarrollo y soporte: Para garantizar la seguridad de la información que se ha diseñado e implementado dentro del ciclo de vida de desarrollo de sistemas de información.	A.14.2.1 Política de desarrollo seguro	Se deben establecer reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	N	N	Gestión de IT	Sitech de Colombia no realiza desarrollos de software internos
				A.14.2.2 Procedimientos de control de cambios en sistemas	Los cambios en los sistemas dentro del ciclo de desarrollo deberán controlarse mediante el uso de procedimientos formales de control de cambios.	N	N	Gestión de IT	Dado que Sitech de Colombia no realiza desarrollo no es necesario implementar mecanismos de control durante el ciclo de desarrollo del software
				A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no hay impacto adverso sobre las operaciones o la seguridad de la organización.	S	N	Gestión de IT	
				A.14.2.4 Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	S	N	Gestión de IT	
				A.14.2.5 Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	S	N	Gestión de IT	
				A.14.2.6 Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que cubren todo el ciclo de vida de desarrollo de sistemas.	N	N	Gestión de IT	Sitech de Colombia no realiza desarrollos de software internos

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
				A.14.2.7 Desarrollo contratado externamente	La organización debe supervisar y controlar la actividad de desarrollo de sistemas fuera de origen.	S	S	Gestión de IT	
				A.14.2.8 Pruebas de seguridad de sistemas	Pruebas de funcionalidad de la seguridad se deben llevar a cabo durante el desarrollo.	N	N	Gestión de IT	Sitech de Colombia no realiza desarrollos de software internos
				A.14.2.9 Prueba de aceptación de sistemas.	Para los nuevos sistemas de información, actualizaciones y nuevas versiones se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	S	N	Gestión de IT	
		A.14.3	Datos de prueba: Para garantizar la protección de los datos utilizados para la prueba.	A.14.3.1 Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	S	N	Gestión de IT	
A.15	Relaciones con los proveedores	A.15.1	Seguridad de la información en las relaciones con los proveedores: Para garantizar la protección de los activos de la organización que sea accesible por los proveedores.	A.15.1.1 Seguridad de la información en las relaciones con los proveedores	Los Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, se deben acordar con estos y se deben documentar.	S	N	Todos	
				A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de las organizaciones.	S	N	Todos	
				A.15.1.3 Cadena de suministro de tecnología de información y comunicación.	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	S	N	Área Logística	
		A.15.2	Gestión de la prestación de servicio de proveedores: Para mantener un nivel acordado de seguridad de la información y la	A.15.2.1 Seguimiento y revisión de los servicios de proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	S	S	Todos	
				A.15.2.2 Gestión	Se deben gestionar los cambios en el	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
			prestación de servicios en línea con los acuerdos con proveedores.	de cambios en los servicios de proveedores	suministro de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información comercial, los sistemas y los procesos del negocio involucrados y la reevaluación de los riesgos.				
A.16	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información: Para garantizar un enfoque coherente y eficaz para la gestión de los incidentes de seguridad de la información, incluida la comunicación de eventos y debilidades de seguridad.	A.16.1.1 Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	S	N	Todos	
				A.16.1.2 Reporte de eventos de seguridad de información	Los eventos de seguridad de la información deben ser reportados por la vía de administración adecuada tan pronto como sea posible.	S	N	Todos	
				A.16.1.3 Reporte de debilidades de seguridad de información	Se debe exigir a todos los empleados y contratistas que utilizan sistemas y servicios de información de la organización, que observen y reporten cualquier deficiencia de seguridad de información detectada o sospechada en los sistemas o servicios.	S	N	Todos	
				A.16.1.4 Evaluación de eventos de seguridad de información y decisión sobre ellos.	Los eventos de seguridad de la información deben ser evaluados y se debe decidir si han de ser clasificados como incidentes de seguridad de la información.	S	N	Todos	
				A.16.1.5 Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deberán recibir una respuesta de acuerdo con los procedimientos documentados.	S	N	Todos	
				A.16.1.6 Aprender de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de los incidentes de seguridad de la información se debe utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.	S	N	Todos	
				A.16.1.7 Recolección de evidencias	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
					información, que puede servir como evidencia.				
A.17	Aspectos de seguridad de información de la gestión de continuidad del negocio	A.17.1	Continuidad de seguridad de la información la continuidad de la seguridad de la información deben ser incorporados en los sistemas de gestión de continuidad de negocio de la organización.	A.17.1.1 Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	S	S	Todos	
				A.17.1.2 Implementación de la continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.	S	N	Todos	
				A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar la continuidad de los controles de seguridad de información establecidos y aplicados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.	S	N	Todos	
		A.17.2	Redundancias: Para garantizar la disponibilidad de las instalaciones de procesamiento de información.	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	S	N	Todos	
A.18	Revisiones de seguridad de la información	A.18.1	Cumplimiento: Para evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualesquiera requisitos de seguridad.	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	Todo los requisitos estatutarios, reglamentarios, contractuales, regulatorios y el enfoque de la organización para cumplir con estos requisitos deberán ser identificados de forma explícita, documentados y actualizados, para cada sistema de información y la para la organización.	S	S	Todos	
				A.18.1.2 Derechos de propiedad intelectual	Se deben implementar procedimientos adecuados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario.	S	S	Todos	
				A.18.1.3 Protección de registros	Los registros deben ser protegidos de la pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, de conformidad con los requisitos legislativos,	S	N	Todos	

Clausula		Objetivo		Control		Aplica (S/N)	Control implementado (S/N)	Dueño de proceso / Responsable	Razón de No Aplicabilidad
					reglamentarios, contractuales y comerciales.				
				A.18.1.4 Privacidad y protección de información de datos personales	Se debe proteger la privacidad y protección de datos personales como se requiere en la legislación y reglamentación pertinente.	S	S	Todos	
				A.18.1.5 Reglamentación de controles criptográficos	Controles criptográficos Deben ser utilizados en el cumplimiento de todos los acuerdos pertinentes, leyes y reglamentos.	S	N	Gestión de IT	
		A.18.2	Revisiones de seguridad de la información: Para asegurarse que la seguridad informática es implementada y operada de acuerdo con las políticas y procedimientos de la organización.	A.18.2.1 Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se deben revisar de forma independiente a intervalos planificados o cuando se producen cambios significativos.	S	N	Alta Dirección	
				A.18.2.2 Cumplimiento con las políticas y normas de seguridad	Los directores deberán revisar periódicamente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad, con las políticas de seguridad, y cualquier otro requisito de seguridad.	S	N	Alta Dirección	
				A.18.2.3 Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente para determinar el cumplimiento de las políticas y normas de seguridad de la información de la organización.	S	N	Alta Dirección	

Anexo H. Control de visitantes al cuarto de comunicaciones

SITECH SOLUCIONES EN TECNOLOGÍA	**CONTROL DE VISITANTES AL CUARTO DE COMUNICACIONES**	**Código** PENDIENTE **Versión** 1 de 1 **Fecha** 31/07/16 **Página** 1 de 1

FECHA	HORA DE ENTRADA	NOMBRE VISITANTE	No. DOCUMENTO DE IDENTIDAD	EMPRESA O DEPARTAMENTO	MOTIVO DE VISITA	FIRMA VISITANTE	HORA DE SALIDA	FUNCIONARIO QUE AUTORIZA INGRESO AL C.C.